NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

POLICY OPTIONS TO ADDRESS CRUCIAL COMMUNICATION GAPS IN THE INCIDENT COMMAND SYSTEM

by

Edward Bushman

September 2012

Thesis Advisor:	Nadav Morag
Second Reader:	Roxanne Bercik

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2012	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Policy Options to Address Crucial Communication Gaps in the Incident Command System		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Edward Bushman			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number _____N/A_____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

The Incident Command System (ICS) resulted from the need for a new approach to the problem of managing wildfires in the early 1970s. The events of September 11, 2001, led to issuing of Homeland Security Presidential Directive (HSPD) 5 requiring agencies to adopt ICS as their incident management system. However, in events of national significance since then, internal communications have not performed well, causing numerous response problems. In addition, public information systems have failed to meet the community's expectations and keep the public informed about the size, scope, and impact of the emergency.

Three models of possible solutions for addressing the problem were assessed. Model 1 consists of expanding the Communications Unit within the Logistics Section. Model 2 expands and clearly defines the duties, roles and responsibilities of the Public Information Officer. Model 3 merges all communications functions into one section directly under the Incident Commander. Metrics were designed around the management characteristics of the ICS and were assessed utilizing a defined scale.

The research found that the creation of the Communication Section would provide the most benefits towards improving communications. However, that model may be difficult to implement due to resistance to strategic change.

14. SUBJECT TERMS Incident Command System, ICS, National Incident Management System, NIMS, Communications,			**15. NUMBER OF PAGES** 141
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

POLICY OPTIONS TO ADDRESS CRUCIAL COMMUNICATION GAPS IN THE INCIDENT COMMAND SYSTEM

Edward Bushman
Battalion Chief, Los Angeles Fire Department
B.S., University of Redlands, 1995

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
September 2012**

Author: Edward Bushman

Approved by: Nadav Morag
Thesis Advisor

Roxanne Bercik
Second Reader

Daniel Moran
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Incident Command System (ICS) resulted from the need for a new approach to the problem of managing wildfires in the early 1970s. The events of September 11, 2001, led to issuing of Homeland Security Presidential Directive (HSPD) 5 requiring agencies to adopt ICS as their incident management system. However, in events of national significance since then, internal communications have not performed well, causing numerous response problems. In addition, public information systems have failed to meet the community's expectations and keep the public informed about the size, scope, and impact of the emergency.

Three models of possible solutions for addressing the problem were assessed. Model 1 consists of expanding the Communications Unit within the Logistics Section. Model 2 expands and clearly defines the duties, roles and responsibilities of the Public Information Officer. Model 3 merges all communications functions into one section directly under the Incident Commander. Metrics were designed around the management characteristics of the ICS and were assessed utilizing a defined scale.

The research found that the creation of the Communication Section would provide the most benefits towards improving communications. However, that model may be difficult to implement due to resistance to strategic change.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AFAC	Australasian Fire Authorities Council
AIIMS	Australasian Inter-Service Incident Management System
BIA	Bureau of Indian Affairs
BLM	Bureau of Land Management
CDF	California Department of Forestry and Fire Protection
COML	Communications Unit Leader
COMT	Communication Technician
EBRPD	East Bay Regional Parks District
EMS	Emergency Medical Services
EOC	Emergency Operations Center
FEMA	Federal Emergency Management Agency
FGC	Fire Ground Command
FIM	Field Information Manger
FIRESCOPE	Firefighting Resources of Southern California Organized for Potential Emergencies
FRP	Federal Response Plan
FWS	Fish and Wildlife Service
GIS	Global Information Systems
GPS	Global Position System
HSPD	Homeland Security Presidential Directive
IAP	Incident Action Plan
IC	Incident Commander
ICP	Incident Command Post
ICS	Incident Command System
IDM	Information Dissemination Manager
IGM	Information Gathering Manager
IMS	Incident Management System
JIC	Joint Information Center
JIS	Joint Information Systems
LEICS	Law Enforcement Incident Command System
MACS	Multiagency Coordination System
MBO	Management By Objectives
NCP	National Oil and Hazardous Substances Pollution Contingency Plan
NGO	Non-governmental Organizations

NIC	National Integration Center
NIIMS	National Interagency Incident Management System
NIMS	National Incident Management System
NIOSH	National Institute for Occupational Health and Safety
NPS	National Park Service
NRF	National Response Framework
NRP	National Response Plan
NSW	New South Wales
NWCG	National Wildfire Coordinating Group
OES	California Governor's Office of Emergency Services
PIO	Public Information Officer
POST	Police Officers Standards and Testing
RADO	Radio Operator
SEMS	Standardized Emergency Management System
SFFD	San Francisco Fire Department
SSM	Soft Systems Methodology
UC	Unified Command
US&R	Urban Search and Rescue
VIP	Very Important Person
VOIP	Voice Over Internet Protocol

ACKNOWLEDGMENTS

I would like to begin by thanking my family for the love and support they have provided. This thesis is dedicated to my lovely wife, Eve and daughter Samantha, as a humble offering of gratitude for serving as my first, and best, supporters. To my wife Eve—my best friend, whose love and support is priceless—thank you. Samantha, I offer my love and appreciation and hope that this thesis can be an example of a far goal that can be accomplished with dedication and hard work. Your patience and understanding has meant the world to me. The waiting is over; now there are interesting places to go and fresh challenges ahead and I could not ask for a better family to explore them with.

To my mother and sister, thank you for your everlasting support, and instilling me with a love of learning and sense of duty to my community which led me to choosing a career in public service.

I would like to express my gratitude to the Los Angeles Fire Department for supporting my participation in this program. Special thanks to my colleagues in the Homeland Security Division and Battalion 4 who have been my cheering section for the past 18 months. It really made a difference. The citizens of Los Angeles rarely realize the assets they possess in the men and women of the LAFD.

I also wish to express my appreciation to the instructors and staff at the Center for Homeland Defense and Security. Every one of the instructors deserves recognition for the outstanding discussions and challenging atmosphere. Individual acknowledgement, appreciation and thanks go to my advisor Nadav Morag for believing in me, and pushing to bring these ideas to print. In addition, thanks to Deputy Chief Roxanne Bercik. Somehow, she was convinced that I was capable of more. Thanks you to my editor, Pam Silva who took a rough compilation and turned it into a complete thesis. Finally, thank you to my peers. The many hours of spirited debates have expanded my knowledge vastly, and challenged me to see new perspectives that help me daily in my work. I am humbled and honored to have sat among you, and I am privileged to call you my friends.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

> In Homeland security presidential directive (HSPD) 5- Management of Domestic incidents, the President directed me to develop, submit for review to the Homeland Security Council, and administer a National Incident Management System. This system will provide a consistent nationwide approach for Federal, State, Local and tribal governments to work effectively and efficiently together to prepare for, prevent, respond to, and recover from domestic incidents regardless of the cause, size, or complexity
>
> Tom Ridge, 2004[1]

A. BACKGROUND—THE INCIDENT COMMAND SYSTEM

The Incident Command System (ICS) resulted from the obvious need for a new approach to the problem of managing rapidly moving wildfires in the early 1970s. At the time, emergency managers faced a number of problems in managing large, complex or expanding incidents. These included too many people reporting to one supervisor, different emergency response organizational structures, lack of reliable incident information, inadequate and incompatible communications, and unclear lines of authority.

Emergency management and incident management refer to the broad spectrum of activities and organizations providing effective and efficient operations, coordination, and support.[2] Emergency management describes the science of managing complex systems and multidisciplinary personnel to address events and incidents, across all hazards, and through the phases of mitigation, preparedness, response, and recovery. Incident management, by contrast, includes acquiring, coordinating, and delivering resources to incident sites; directing specific incident operations; and sharing information about the incident with the public. Response activities directly address the hazard impact,

[1] Department of Homeland Security. "*National Incident Management System*," 2004, 5.

[2] Ibid., 15.

including actions taken in anticipation of an impending event (e.g., hurricane, tornado) and actions during and after an impact has occurred.

In 13 days of fire in 1970, 16 lives were lost, 700 structures were destroyed and 500,000 acres were burned. Much of this occurred within the jurisdictions of the Los Angeles City and Los Angeles County fire departments. Post-incident critiques indicated that while both departments cooperated with each other, their joint effectiveness did not meet the expectations of either agency. Shortly thereafter, responding to catastrophic fires throughout California, with similar post-incident critiques, Congress tasked the U.S Forest Service with the goal of improving incident management and resource coordination aimed specifically at wildland fires. Designing a standard incident management system to remedy the problems took several years and field-testing. Development of the system took an inter-agency task force with cooperating local, state, and federal efforts. The early developmental process recognized and keyed on several requirements for the system that exists today. These requirements were that the system must be organizationally flexible to meet the needs of incidents of any kind and size; agencies must be able to use the system on a day-to-day basis for routine situations as well as for major emergencies; it must be sufficiently standard to allow personnel from a variety of agencies and diverse geographical locations to rapidly meld into a common management structure, and it must be cost-effective.

The result was the ICS. Initial ICS applications were designed for responding to wildland fires. However, the characteristics of these wildland fire incidents was found to be similar to those seen in many law enforcement, hazardous materials and other kinds of situations, and ICS became an all-hazards system.

Public safety agencies saw the benefits of the ICS and of a single incident management system and the adoption of ICS spread. The adoption was facilitated on occasions due to catastrophic events. The events of September 11, 2001, and the resulting after action reports led to the president issuing Homeland Security Presidential Directive

(HSPD) 5 on February 28, 2003.[3] The effective result of HSPD 5 was that all agencies adopted the National Incident Management System (NIMS) and ICS as their incident management system.

When coping with a natural disaster, wildfire, disease outbreak or any other incident, agencies at the local, state, and federal levels have to effectively communicate, coordinate operations, and allocate resources. ICS is the approach to be used by those agencies to assemble and control the temporary systems they employ to manage personnel and equipment at emergencies. The ICS is a tiered system. The organizational layers are used only when appropriate and only as dictated by system complexity. The highest management level is the incident commander, command staff, which includes the management staff and the general staff of four functional section chiefs. The ICS is built around the five functions of management, command, planning, operations, logistics, and finance. (Intelligence/Investigations is an optional sixth functional area that may be activated on a case-by-case basis.) The ICS, Multiagency Coordination System (MACS), and public information are the fundamental elements of incident management.[4]

ICS has important strengths in organizing emergency response. It factors critical emergency tasks, establishing a clear division of labor and assignment of functional responsibility. It defines the chain-of-command, provides a manageable span of control for each function, and establishes a resource allocation, decision-making structure that is critically important to avoid dispute about "who is in charge" and to enable rapid deployment and direction of personnel and equipment. It is designed to promote information flows up, down, and across the organization and to the public. As a result, ICS is highly flexible in response to any incident type, scale, and location.

From the very beginning, the major fire departments in California that were committed to the concept realized that ICS must be used on a daily basis to be successful.[5] For firefighters, ICS was a necessary invention that addressed core

[3] Homeland Security Presidential Directive 5, February 28, 2003.

[4] Department of Homeland Security, "*National Incident Management System.*" 2008. 6.

[5] "National Incident Management System Consortium," http://www.ims-consortium.org/backinfo.htm.

professional problems. It made good sense to train and exercise all personnel in the system and use it regularly, even to respond to small events. ICS became virtually second nature when events made it essential. For law enforcement in the U.S., by contrast, adoption was less enthusiastic. Comparing policing to firefighting, one notes that active field co-ordination involving significant numbers of police officers occurs much less regularly. Although it does occur, for example, in security for large events, hostage takings, and drug busts. Collaboration with mutual aid providers from other jurisdictions is quite rare. Hence, the need for ICS would seem less compelling; and the costs of preparing personnel and the organization as a whole may seem more burdensome, perhaps unjustified.[6]

B. PROBLEM STATEMENT

The ICS is not meeting the current needs of the citizens. The ICS was developed in the 1970s; since then, it has undergone few changes or modifications. ICS is a complex system with numerous components including structure, training and implementation. ICS has many aspects, but the communication aspect needs current attention. The focus of this paper is the communications problems. Communications problems in the ICS have not given the incident commander full situational awareness of the emergency. This issue prevents effective plans, inhibits response, and endangers responders and the public.

In events of national significance since its adoption in 2004, inter-incident or internal communications have not performed well, causing numerous response problems. As more accounts of decision making during Katrina become part of the public record, it becomes apparent that major shortcomings of situational awareness resulted because information about conditions was unavailable and/or did not reach senior decision makers.[7]

---

[6] Arnold Howitt and Herman B. Leonard, "A Command System for All Agencies?" *Crisis/Response Journal.* March 2005, 40–42.

[7] Ibid., "Beyond Katrina: Improving Disaster Response Capabilities" *Crisis/Response Journal.* September 2006.

In addition, external communications or public information systems have failed to meet the community's expectations and keep the public informed about the size, scope, and impact of the emergency. As stated in Congressional hearings regarding the Deepwater Horizon spill, the flow of information was poor. Craig Paul Taffaro Jr., president of St. Bernard Parish, stated, "The information presented by BP in print and broadcast media often erupted into episodes of frustration and disbelief as the disconnect between the reality of a local experience and the stated information was clearly displayed."[8] From the breaking notice that an explosion had occurred, the information was wrought with inconsistencies, fragmented messaging, and stove-piped communication patterns. The challenge to share information was never conquered.[9]

Also, since the creation of the ICS, society and society's expectations of emergency management have changed. These societal changes include technology enhancements and innovations. The uses of Internet information technologies have created new expectations among our citizens. They are demanding to be informed, and warned of impending danger. In some cases, warnings can be more important that response and can protect more lives. These failures of the ICS create increased impact from hurricanes, fires, floods, and other emergency incidents by reducing the efficiency of the management system. In addition, the public is increasingly uninformed as to the incident, their expected actions, and threats to public safety. The ultimate effect is that the public is adversely impacted due to the incident management's deficiencies. The ability to enhance the effectiveness of incident management may serve to minimize the impact of such events.

The problem centers on the ICS and or its implementation. Questions arise if the problem is centered on a structural deficiency of the ICS, or whether it is an implementation and training issue. It is important to realize that, from a design perspective, the form of the ICS system is a normative concept; it specifies how

---

[8] Committee on Homeland Security: Hearings on Preliminary the Lessons from Deepwater Horizon. 111th Cong. (2010). September 22, 2010. Serial No. 111–80. Statement of Mr. Craig Paul Taffaro, Jr., St. Bernard Parish, Louisiana.

[9] Ibid.

command and control should be performed according to the design. There is, of course, no guarantee that command and control will be performed in that way. It is therefore important to distinguish between the form of the ICS, which specifies how command and control should be performed, and the process of incident management and the "culture," which denotes how it actually is performed.

This paper does not explore the market penetration of the ICS or the appropriateness of the implementation and training regime. This paper focuses on the structural issues with the ICS, which facilitate or detract from effective communication. Specifically, this paper has narrowed the scope of the problem to focus on structural deficiencies in the ICS that cause incident communications, including internal communications and external communications (public information) problems. The problem is that internal communication policies, procedures, and systems have failed to keep leaders informed of the size and scope of the emergencies. This has led to poor decision making by incident commanders and other response problems. In addition, public information (external communications) has failed to keep the citizens informed about the size, scope and impact of the emergency. This creates additional risks to stakeholders and the public, due to missed evacuation warnings or other critical information.

This thesis is organized in the following manner: Chapter II explores the history of the ICS. It identifies the beginnings in the California fire service to the present. Chapter II also identifies many of the milestones in the development of the ICS, the incidents that provoked its adoption and how the ICS has evolved. It shows that the ICS was constantly reviewed to ensure that the system met the needs of stakeholders. Through this, we must assume that this evolution is not final and that ICS will continue to be assessed to ensure that it is meeting current expectations.

Chapter III presents a literature review of the ICS. The literature review focuses on federal literature, literature on the growth and maturation of the ICS, and scholarly literature.

Chapter IV further defines the problem and discusses the research questions. The research questions to be studied are:

1. Which type of structure would make communications in the ICS more efficient?

2. Are internal (incident communications) and external communications (public information) related sufficiently so that they can be combined within the ICS?

3. Or, do internal and external communications need to remain separated to operate efficiently?

4. Would the changing the ICS communications structure meet the community's current expectations?

In addition, Chapter IV explores the research methodology. In order to fully assess and answer the research questions, a Soft systems methodology is utilized. Soft systems methodology (SSM) is a systemic approach for tackling real-world problematic situations. Soft systems methodology (SSM) was developed by Peter Checkland and his colleagues at Lancaster University in the 1970s. It is designed to shape interventions in the problematic situations encountered in management, organizational, and policy contexts. Though informed by systems engineering approaches, it breaks with them by recognizing the central importance of perspective or world-view in social situations. It differs significantly from the "systems science" approaches developed in the 1960s, and is more reflective of action research in its philosophy and approach.[10]

The key components of the SSM are:

1. Identifying a real-world situation seen as calling for action to improve it;

2. Developing models of purposeful activity relevant to this situation;

3. Identifying a process of using the models as devices to explore the problem;

[10] Stan Lester, "Soft System Methodology." Available at http://www.sld.demon.co.uk/ssm.pdf.

4. Conducting a structured debate about the desirable and feasible change.[11]

The three models of purposeful activity are possible solutions for addressing the ICS communications problem. Each would involve restructuring the incident command system to make communications a priority. Restructuring may take alternative forms and each contains drawbacks.

1. Expanding the Communications Unit Within Logistics

This model would expand the Communications Unit within the Logistics, Service Branch to include all current and future internal communications functions. The Public Information Officer remains on the incident commander's command staff and the function of public information remains as is. The expanded Communication Unit's job functions would be defined to include all of the incident's current and future expectations.

The Communications Unit will be required to define new positions to encompass the new responsibilities and emerging technologies networking capabilities

2. Expanding the Public Information Officer Role

In Model 2, external communication will continue to be handled by the Public Information Officer (PIO). The PIO would continue to support the incident command structure as a member of the command staff and advise the incident commander/unified commander on all public information matters relating to the management of the incident. The position would be given specific responsibilities and tasks that the defined PIO would be required to complete. This option would keep the internal communication support functions within the Communications Unit within Logistics

The PIO may be assigned assistant PIOs as allowed under ICS. However, these assistants will have duties and responsibilities defined to meet the expanding communication requirements. These requirements will ensure that incident information

[11] Peter Checkland and John Poulter, "*Learning For Action: A Short Definitive Account of Soft Systems Methodology, and Its Use Practitioners, Teachers and Students*,"(New Jersey: John Wiley and Sons Ltd. 2007) 11.

reaches the existing people and networks. Social media will be utilized to reach out to the community to deliver warnings and information. In addition, new media will be utilized to bring relevant information from the community to the incident.

3. Creating a Communications Section

The ICS now has four sections: Operations, Planning, Logistics, and Finance. Deep within the Logistics section, under the Support Branch, resides the Communications Unit. External Communication is handled by a member of the command staff, the PIO. While the PIO may have assistants assigned on an as-needed basis, a clear, defined organization is not defined. This model is to merge all communications functions into one section directly under the Incident Commander. Within the Communications Section, all information collection, creation and delivery systems will be combined into one section reporting directly to the Incident Commander.

This section would handle all internal and external communications functions, with each having a separate unit, group, or—if necessary— separate branches.

In identifying a process of using the models as devices to explore the problem, we have returned to the tenants of the ICS. The ICS was designed to adhere to 14 key management concepts. In addition, research has identified five adaptability criteria and four criteria measuring the expectation for success. The criteria are explained in greater detail in Chapter IV. An objective measure of effectiveness of each model would prove difficult since the options would have little opportunities for field testing, thus effectively preventing the collection of a great deal of quantitative data on the benefits of any of the options. Therefore, the criteria for judging the success of each of the options must include an estimate of effectiveness of promoting the primary goal of the ICS, that being to serve the needs of the community, to protect lives, and save property. In addition, measures of effectiveness were judged based on how the options positively or negatively impact the assessment factors.

The models seek changes in the current incident command system and are measured as to how they affect command, control, communication, coordination, and cooperation within the system. A matrix of the tenants of the ICS is utilized and the options are evaluated in each category.

Chapter V describes the models in depth. Each model presents its expected outcomes and its intent to improve incident management communications. Chapter VI begins the structured debate about the desirable and feasible change. Utilizing the matrix developed of the key concepts measured against the models, the research identifies the optimum models to recommend. The recommendations will also have considered the most likely recommendations of success.

Metrics are assessed utilizing a scale of 1 to 9, with 9 offering the most improvement over the current system. A rating of 5 will define a neutral benefit (no change) and 1 will signify a reduction from the current practice.

Chapter VII presents a summary of the findings and final recommendations. In addition, it discusses areas of further study.

C. SIGNIFICANCE OF RESEARCH

The proposed outcome of the research intends to identify an alternative ICS structure that will improve internal and external communications. The benefits of the research could lead to a stronger national response plan and an improved National Incident Management System.

The following chapter begins with the history of the ICS and how it spread from west to east and abroad.

II. HISTORY OF THE INCIDENT COMMAND SYSTEM

> There was a desert wind blowing that night. It was one of those hot dry Santa Anas that come down through the mountain passes and curl your hair and make your nerves jump and your skin itch. On nights like that every booze party ends in a fight. Meek little wives feel the edge of the carving knife and study their husbands' necks. Anything can happen.[12]
>
> Raymond Chandler, Red Wind,

A. CHAPTER INTRODUCTION

This chapter describes the history of the Incident Command System, including. the birth and development, and the reasons it was necessitated. In addition, this chapter discusses some of the major incidents that led to adoption. It tracks the ICS spread from Southern California to the entire State of California and through federal agencies that were the early adopters. This chapter also discusses the development of the ICS in Australia. The development of the Australian ICS is a key parallel to the United States system and the lessons learned from Australia can be applied here. This chapter concludes with incidents of national significance since nationwide adoption and highlight ICS communication issues.

The sun rose over Southern California on September 22, 1970, and the *Los Angeles Times* was predicting another hot, dry day.[13] The 1970 fire season was well under way. During the previous weeks, numerous fires had already burned; under these conditions, the fire danger was high.[14] This day was to be like many others, warming to 90 degrees, dry, with a potential Santa Ana Wind.

Southern California contains a unique geography. Along the edge of California, millions live in communities such as Santa Barbara, moving southward towards Ventura,

---

[12] Raymond Chandler, "*Red Wind*." Available at http://ae-lib.org.ua/texts-c/chandler__red_wind__en.htm. 1.

[13] "Weather." *Los Angeles Times*, September 22, 1970, sec. Part II.

[14] "Santa Ana Winds - Wildfires:" National Oceanic and Atmospheric Administration." http://www.noaawatch.gov/2008/santa_ana.php.

Malibu, Los Angeles, Santa Monica, Long Beach, stretching to San Diego and the Mexican border. To the west lies the Pacific Ocean and to the east lies the Mohave Desert. Normal weather patterns have the sun shining on the Mohave Desert floor, heating the air. This hot air rises, creating an area of lower relative pressure. Normal wind currents will flow from a higher pressure area to a lower pressure. This pressure differential draws in air from the west, thus bringing in air cooled by the Pacific. This cooler air helps maintain a temperate climate for most of Southern California almost year around.[15]

However, occasionally during the fall and early winter, a low pressure system parks itself off the coast and a high pressure system forms over the desert to the east. This reverses the normal wind flow and moves the air westward. The wind moves from the high desert to sea level. As it descends the mountains, it is compressed and increases in temperature.[16]

These hot, and very dry Santa Ana winds—with a relative humidity of 10 to 20 percent or lower—dry out vegetation, increasing the fuel available to feed fires. The gusty winds and eddies of winds swirling through canyons and valleys also fan flames and spread burning embers.[17] The winds are associated with some of the area's largest and deadliest wildfires, including the state's largest fire on record, the Cedar Fire,[18] as well as the Laguna Fire,[19] Old Fire,[20] Esperanza Fire,[21] Santiago Canyon Fire of 1889,[22]

---

15 "Santa Ana Winds - Wildfires:" National Oceanic and Atmospheric Administration." http://www.noaawatch.gov/2008/santa_ana.php.

16 Ibid.

17 Ibid.

18 "Cedar Fire" San Diego Fire-Rescue Department. Available at http://www.sandiego.gov/fire/about/majorfires/2003cedar.shtml.

19 "Laguna Fire 1970 - One of California's Worst Wildfires." Available at http://www.cccarto.com/cal_wildfire/laguna/fire.html, Accessed August 10, 2012.

20 "Old Fire 10-26-03." Available at http://www.incidentcontrol.com/oldfire/index.html.

21 "California Department of Forestry and Fire Protection - *Esperanza Fire*," Available at http://bof.fire.ca.gov/incidents/incidents_details_info?incident_id=161.

22 "Fire Burns in Espraranza." *Los Angeles Times*, September 27, 1889, sec. A

and the Witch Fire.[23] Many years previously, on a similar November morning in 1961, a Sherman Oaks construction crew, working just north of Bel-Air, noticed smoke and flames coming from a nearby pile of rubbish. Within minutes, Santa Ana winds swept burning embers from roof to roof, spreading fire across the affluent enclaves of the Santa Monica Mountains. Before it was contained less than two days later, it destroyed nearly 500 homes worth about $30 million.[24] When Santa Ana winds come, firefighters prepare for the worst and red flags are raised for warning.[25] On September 23, 1970, the Santa Ana winds were here.

By September 27, 1970, 14 major fires were burning out of control. Four separate fires had joined into a single massive fire creating a perimeter from Newhall to Malibu. Thousands fled their homes in advance of the fire. Los Angeles Fire Department Fire Chief Raymond Hill remarked that "we have every piece of civil defense equipment from Monterey to the Mexican border on the front lines." [26]

On September 28, 1970, the Santa Ana winds continued. San Diego County reported a 10-mile long wall of flames forcing 10,000 to flee. Two hundred homes were destroyed and 17 communities were evacuated. In addition, six other fires were reported in San Diego County.[27]

By the end of the 13-day period beginning September 22, 1970, 773 wildfires in Southern California burned 576,508 acres, destroyed 722 homes, and killed 16 people. Although all agencies cooperated to the best of their ability, numerous problems of

---

[23] "California Department of Forestry and Fire Protection - *The Witch Fire*," Available at. http://cdfdata.fire.ca.gov/incidents/incidents_details_info?incident_id=225."

[24] "The Los Angeles Fire Department Historical Society- *The Bel Air Fire - Nov. 6th, 1961*," Available at http://www.lafdmuseum.org/siteblog-post-action/id.22/title.the-bel-air-fire-nov-6th-1961."

[25] "Weather Service Glossary" "National Oceanic and Atmospheric Administration, Available at http://www.weather.gov/glossary/index.php?word=red%20flag%20warning.

[26] Dial Torgerson, "14 Major Fires Rage Out Of Control: 256 Homes Destroyed as Flames Burn 180,000 Acres Some Fight It or Flee It---Others Just Yell Fore! Man Vs. Nature at Her Worst." *Los Angeles Times*, September 27, 1970, sec. A.

[27] Steve Emmons, "Brush Fires Sweep Trabuco, Brea Areas, Force Evacuation: Shifting Winds Ease Threat in County After Flames Scorch Campgrounds, Raze Home, Peril Gasoline Plant." *Los Angeles Times*, September 28, 1970, sec. PART II.

communication and coordination hampered their effectiveness. The Los Angeles County Fire Department had added 30 new fire companies since the disastrous 1958 fires, but the 1970 fires were fought with the same command and control techniques.[28]

After the devastating fire season of 1970, the California fire services were severely criticized for failure to provide leadership in solving the issues of cooperation, command and control, communications, and training. To address the issue, in 1971, the 92nd Congress approved funding for the U.S. Forest Service Research to design a system that will "Make a quantum jump in the capabilities of Southern California wildland fire protection agencies to effectively coordinate interagency action and to allocate suppression resources in dynamic, multiple-fire situations."[29]

This federal legislative action authorized funding for a five-year research program coordinated by the California Governor's Office of Emergency Services (OES). The research began with a group of leaders from California's largest firefighting agencies, including the California Department of Forestry and Fire Protection, the Governor's Office of Emergency Services, Los Angeles, Ventura and the Santa Barbara County Fire Departments, and the Los Angeles City Fire Department. In addition, they were joined with the U.S. Forest Service. The program was named FIRESCOPE (Firefighting Resources of Southern California Organized for Potential Emergencies) and began the joint development of the systems to improve firefighting operations in large-scale incidents.[30] High-ranking administrative/command-level officers representing federal, state and local fire protection agencies in Southern California made up FIRESCOPE's policy board. These officials were of such rank that they could make operational policy decisions for their agencies.[31] Although the original task force's early investigation into multi-agency operations focused on equipment including radio and hose coupling

---

[28] Dial Torgerson, "Can We Prevent Future Disasters?" *Los Angeles Times*, October 4, 1970, sec. A.

[29] "About FIRESCOPE," Available at http://firescope.org/about-us.htm.

[30] " History of ICS." National Training Curriculum, October 1994. Available at http://www.nwcg.gov/pms/forms/compan/history.pdf.

[31] William M. Neville, and Neamy, Robert. "From Firescope to NIMS - The Evolution of the National Incident Management System." *Fire Rescue Magazine*, August 2011.

compatibility, and department emergency operations policies, it soon became obvious to FIRESCOPE members that the primary issues actually revolved around the diverse missions of the involved agencies, and the divergent nomenclature and organizational structures used by the agencies for command of emergency incidents.[32]

FIRESCOPE, utilizing the lessons from the 1970 fires, began to explore the complexity of incident management in a large or expanding incident, coupled with the growing need for multi-agency and multifunctional involvement on incidents. The program's foundation revolved around (1) improving fireground operations, (2) increasing the effectiveness of fire protection agencies, and (3) improving multi-agency coordination. They determined that there was an increased need for a single standard incident management system that can be used by all emergency response disciplines.[33] FIRESCOPE determined that an effective fire management system must contain the following elements:

- Coordinate multi-agency resources during major incidents.
- Develop improved methods for forecasting fire behavior.
- Develop standard terminology.
- Provide multi-agency communications.
- Provide multi-agency training.[34]

These five basic elements were consolidated into two components that would make up the FIRESCOPE system, namely:

- Incident Command System for improving incident management.

---

[32] William M. Neville, and Robert Neamy, "From Firescope to NIMS - The Evolution of the National Incident Management System." *Fire Rescue Magazine*, August 2011.

[33] "Past Present Future.pdf," Available at http://firescope.org/firescope-history/past%20present%20future.pdf.

[34] "About FIRESCOPE," Available at http://firescope.org/about-us.htm. Accessed October 10, 2011.

- Multi-Agency Coordination System (MACS) for improving multi-agency coordination for major or multiple incidents.[35]

The Incident Command System is used to organize on-scene operations for a broad spectrum of emergencies from small to complex incidents, both natural and manmade. The field response level is where emergency management/response personnel, under the command of an appropriate authority, carry out tactical decisions and activities in direct response to an incident or threat. ICS is founded upon a number of key concepts, including:

- Unity of Command (Chain of Command)
- Clear Text (Common Terminology)
- Management by Objective
- Flexible/Modular Organization
- Span-of-Control

Coordination on any incident or event is possible and effective due to the implementation of the following concepts:

- Incident Action Plan
- Comprehensive Resource Management
- Integrated Communications

An incident command system must be able to meet the requirements of an expanding incident, and remain easy to use and flexible to meet the requirements of all types of incidents.[36]

The need for an interagency coordinating mechanism had been recognized long before the 1970 fires. National events had a strong influence in focusing this need. The

35 "Past Present Future.pdf," Available at http://firescope.org/firescope-history/past%20present%20future.pdf.

36 " History of ICS," National Training Curriculum, October 1994. Available at http://www.nwcg.gov/pms/forms/compan/history.pdf.

1973 "America Burning" Task Force Report, which strongly urged a single national firefighting concept that was not to be in the wildland fire community.[37] These issues and the fires of 1970, 1971, and 1973 stimulated the formation of the National Wildfire Coordinating Group.

The National Wildfire Coordinating Group (NWCG) is made up of the USDA Forest Service; four Department of the Interior agencies: Bureau of Land Management (BLM), National Park Service (NPS), Bureau of Indian Affairs (BIA), the Fish and Wildlife Service (FWS); and State forestry agencies through the National Association of State Foresters. The purpose of NWCG was to coordinate programs of the participating wildfire management agencies so as to avoid wasteful duplication and to provide a means of constructively working together. The NWCG provided a formalized system to agree upon standards of training, equipment, qualifications, and other operational functions.[38]

By 1976, the FIRESCOPE agencies formally agreed on ICS common terminology and procedures. The ICS was born. Later that year, limited field-testing began. By 1978, parts of the ICS were successfully used on several wildland fire incidents and applied to urban firefighting. That year, ICS was formally adopted by the Los Angeles City Fire Department as the incident management structure for all incidents. Another key component of the Multi-Agency Coordination System (MACS) was approved that same year.[39]

ICS was formally adopted by the California Department of Forestry and Fire Protection (CDF), the Governor's Office of Emergency Services (OES), partner agencies, and endorsed by the State Board of Fire Services in 1980. In addition, a FIRESCOPE ICS training course development began with the objective of satisfying the needs of local,

---

[37] "United States Fire Administration "*America Burning,*" September 7, 1972, Available at http://www.usfa.fema.gov/downloads/pdf/publications/fa-264.pdf. 97.

[38] Dale D Rowley, "The Fires That Created an IMS.pdf," Available at. http://www.uninets.net/~dsrowley/The%20Fires%20that%20Created%20an%20IMS.pdf. Accessed July 15, 2012.

[39] "Some Highlights of the Evolution of the Incident Command System," Available at http://www.firescope.org/firescope-history/Some%20Highlights%20of%20the%20Evolution%20of%20the%20ICS.pdf.

state and federal agencies. In 1980, the National Wildfire Coordinating Group (NWCG) began to perform an analysis of ICS for possible national application.[40]

In 1981, adaptation of ICS began to expand and create wide use throughout Southern California by major fire agencies. CDF and the OES and the California State Fire Marshal all signed a "Statement of Intent," establishing a mutual commitment to support FIRESCOPE and the ICS Program. Also, many agencies began to utilize ICS on non-fire incidents. Also, the FIRESCOPE Board of Directors approved a response to NWCG, which generally supported the national adoption of a uniform emergency management organization, referred to, as the National Interagency Incident Management System (NIIMS). NIIMS contains basically the FIRESCOPE ICS.[41]

In 1982, the NWCG forwarded and accepted the recommendation for developing the ICS for national application, and the U.S. Forest Service approved implementation of ICS in the Pacific Southwest Region (Region 5) by 1983, and service-wide use by 1985.[42]

1. First Interstate Fire

On Wednesday, May 4, and continuing into May 5, 1988, the Los Angeles City Fire Department responded to and extinguished the most challenging and difficult highrise fire in the city's history. The fire destroyed four floors and damaged a fifth floor of the modern 62-story First Interstate Bank building in downtown Los Angeles. The fire claimed one life, injured approximately 35 occupants and 14 fire personnel, and resulted in a property loss of over $50 million. [43]

A total of 383 Los Angeles City Fire Department members from 64 companies, nearly one-half of the on-duty force of the entire city, were involved in fighting the fire,

---

[40] "Some Highlights of the Evolution of the Incident Command System," Available at http://www.firescope.org/firescope-history/Some%20Highlights%20of%20the%20Evolution%20of%20the%20ICS.pdf.

[41] Ibid.

[42] Ibid.

[43] "The First Interstate Bank Fire," Available at http://www.drj.com/drworld/content/w1_119.htm.

mounting an offensive attack via four stairways. This operation involved many unusual challenges, but is most notable for the sheer magnitude of the fire and the fact that the fire was successfully controlled by interior suppression efforts.

The Highrise Incident Command System was initiated, with companies assigned to fire attack, and to logistics and support functions from the outset. The U.S. Fire Administration report stated that the Highrise Incident Command System was very effective in managing the incident. Despite the massive numbers of companies and firefighters on the scene, the fire department maintained good organization at the scene and effectively—and safely—managed their resources.[44]

Concurrent to the development of ICS, Fire Chief Alan Brunacini was developing the Fire Ground Command (FGC) System in Phoenix, Arizona. The system emphasized structural firefighting applications and other urban-related emergencies such as hazardous materials, mass casualty, and other incident types. The National Fire Protection Association adopted FGC and published several related training materials.

Throughout the 1980s, fire service leaders debated the benefits of each system and the possibilities of merging the best components of the two into a single system. During the 1989 International Association of Fire Chiefs annual conference in Indianapolis, a panel discussion was conducted on the merger possibilities. Based on comments from the audience, there appeared to be strong support for a merger

In July 1990, the first of a series of committee meetings was held with Phoenix Fire Department and FIRESCOPE representatives. In attendance were representatives from the National Fire Academy. Additional committee meetings were held in September 1990 and January 1991. A pivotal meeting between the committee and the FIRESCOPE board of directors occurred in August 1991. As additional meetings occurred, more and more fire service organizations participated, thus increasing representation. During the August 1991 meeting, the committee was re-organized into a more formalized organization. The organization selected the title “National Fire Service Incident

[44] “The First Interstate Bank Fire,” Available at http://www.drj.com/drworld/content/w1_119.htm.

Management System Consortium" (NIMS Consortium) to better describe the organization's mission. During February 1993, the NIMS Consortium completed the successful merger of ICS and FGC. The title "Incident Management System (IMS)" was chosen to identify the merger.[45] The NIMS Consortium and FIRESCOPE continue to have members sit on each others respective boards to ensure collaboration.

2. Law Enforcement

ICS existed for nearly ten years before the law enforcement community began to study and embrace the concept. In the early 1980s, law enforcement leaders in Southern California recognized the benefit of adapting the fire service's ICS to meet the needs of large-scale law enforcement activities. The Police Officers Standards and Testing (POST) organization sanctioned the Law Enforcement ICS (LEICS) development, providing reimbursement for LEICS classes taught to law enforcement personnel.[46] The first major incident management under LEICS was a Pacific Southwest Airlines plane crash in a rural part of San Luis Obispo County.[47] Sheriff's personnel credited LEICS for its ability to manage this event, involving law, fire, and medical personnel from a variety of jurisdictions. LEICS became the basis for the law enforcement and public safety services planning for the 1984 Los Angeles Olympic Games. This Olympics involved more than one hundred local law enforcement agencies, and more than a dozen federal law and military organizations.[48]

Law enforcement agencies generally do not face emergencies of such enormous scale; police agencies seldom must provide such extensive mutual aid to each other. As a result, many law enforcement managers understandably view their incident response

---

[45] National Incident Management System Consortium," Available at http://www.ims-consortium.org/backinfo.htm.

[46] Hank Christen, Paul Maniscalco, Alan Vickery, and Frances Winslow, "An Overview of Incident Management Systems," September 2001, Available at http://www.hcanj.org/docs/An_Overview_of_Incident_Management_Systems.pdf.

[47] "AirDisaster.Com: Special Report: PSA Flight 1771," Available at http://www.airdisaster.com/special/special-pa1771.shtml.

[48] Hank Christen, Paul Maniscalco, Alan Vickery, and Frances Winslow. "An Overview of Incident Management Systems," September 2001, Available at http://www.hcanj.org/docs/An_Overview_of_Incident_Management_Systems.pdf.

systems, often developed in isolation from one another, as effective. However, the 1984 Los Angeles Olympics and subsequent events, both planned and spontaneous, stimulated progressive law enforcement leaders to search for more efficient ways to integrate not only allied police agencies but also other disciplines, such as fire and EMS, at the scene of a crisis. While an individual agency's protocols and procedures may have worked well for years, the need for some standardization quickly became apparent when agencies were forced to integrate their resources rapidly during the response to a major incident.[49]

3. Oakland Hills Fire

Between 1986 and 1991, most of California experienced drought conditions. This situation was recognized as creating more and more critical fire risk conditions each year. The drought conditions prevailed through October 1991 with warmer than normal temperatures. On Saturday, October 19, 1991, the weather was warm, clear, and dry, with no appreciable wind. At 1212 hours, a brush fire was reported on the hillside in the East Bay Hills Fire, near Oakland, California. The fire was attacked from the lower side by Oakland Fire Department fire companies on Buckingham and Westmoorland and from above by companies on Marlborough Terrace. The tactics were successful and the fire was declared under control at 1339 hours. The fire area was limited to two acres, with no structural involvement, and it was stopped on the uphill slope, before reaching the top of the hill.[50]

A Diablo wind condition was predicted for Sunday, October 20, and red flag warnings were issued to area fire agencies.[51] The coastal areas of southern California are extremely vulnerable to the infamous Santa Ana wind. A similar condition occurs in the Oakland area, where it is known as a Diablo (or "Devil") wind. These winds are created

---

[49] Hank Christen, Paul Maniscalco, Alan Vickery, and Frances Winslow, "An Overview of Incident Management Systems," September 2001, Available at http://www.hcanj.org/docs/An_Overview_of_Incident_Management_Systems.pdf.

[50] United Stated Fire Administration/Technical Report Series "*The East Bay Hills Fire*," Available at http://www.usfa.fema.gov/downloads/pdf/publications/tr-060.pdf.

[51] Ibid.

when a high-pressure weather system is located over the great basin of the inland western States, accompanied by an offshore low-pressure system.[52]

Sunday morning, October 20, brought the classic Diablo wind conditions to the Oakland area. The Oakland Fire Department assistant chief, who had also worked the previous day's fire, recognized the danger and directed two engine companies to check the burn area. Arriving at the top of the hill, at 0913, he advised Oakland Fire Communications to again call East Bay Regional Parks and request their assistance in overhauling several hot spots that were flaring-up on the hillside. East Bay Regional Parks District (EBRPD) has its own career fire department and participates in the mutual aid system.

The Oakland and EBRPD units were having difficulty coordinating their efforts, since each agency's units were on their own radio channels. Passing messages via the dispatchers, then by telephone from one communications center to the other, proved to be a problem. The units from both agencies were directed to use the "White" (mutual aid) channel to communicate directly. Between 1040 and 1050 hours, the wind velocity increased and several additional flare-ups were observed; the crews were kept busy moving up and down the steep slope to cover them. Very suddenly, the fire flared up in an unburned area on the lower east flank of the burn area. Burning embers had been carried from one of the hot spots into a patch of timber dry brush. The fire was spreading rapidly uphill, and the strong wind coming over the ridge was pushing the flames out to both flanks at the same time.

Between 1119 and 1125 hours the situation became even worse The fire was spreading south and east on the right flank toward a cluster of homes on Grizzly Peak Terrace The incident commander called for the fifth and sixth alarms at 1120 hours. At 1133 hours, the incident commander instructed Oakland Fire Communications to request

[52] United Stated Fire Administration/Technical Report Series "*The East Bay Hills Fire*," Available at http://www.usfa.fema.gov/downloads/pdf/publications/tr-060.pdf.

five strike teams from Alameda County. He reported that the fire was totally out of control and moving on several fronts, involving more than 100 acres of trees, brush, and houses.

The strike teams that had been requested earlier were beginning to arrive by 1300 hours. Most had difficulty reaching their assigned destinations and establishing contact with the command structure. At 1359 hours, Oakland requested 13 additional strike teams, 6 air tankers, and 6 helicopter attack units. Around 1600 hours, implementation of the ICS on a large scale began to bring the incident into focus at the command post. Prior to this point, Oakland and Berkeley had each operated independently, with their own command posts.

The fire spread rapidly throughout the day and only slowed as the day ended and the winds died down. This allowed some situational awareness to be obtained. Crews continued to contain the fire through the next days with some crews remaining on the lines continuously.

The fire was declared as contained on Tuesday morning. After the full area was surveyed for damage assessment, the number of people left homeless was estimated at close to 10,000, and damage estimates exceeded $1.5 billion. The actual number of structures destroyed was eventually determined to be 3,354 single family dwellings and 456 apartment units. Approximately 2,000 burned vehicles were also located in the area. In the end, 25 lives were lost, including a battalion chief and a police officer.

The management of an incident of this size and complexity was a tremendous challenge. From the beginning of the incident, the situation expanded and changed more rapidly than the suppression forces could communicate, obtain reinforcements, and get organized. Almost 800 structures were ignited within the first hour and more than 300 per hour for the next seven hours. These factors created a situation that exceeded all previous experience with ICS or any other incident management system.

After the Loma Prieta earthquake in 1989, the Oakland Fire Department placed an emphasis on the full implementation of the ICS for managing incidents and coordinating

mutual aid. The ICS was used for this fire, but the shortage of command officers and the extremely fast escalation of the incident made it very difficult to develop the organization in proportion to the situation.

When the fire spread into the city of Berkeley, yet another independent command structure was established, with the Berkeley Fire Department units utilizing their own radio system. This meant that there were two "primary" incident commands and two "secondary" commands, working with four separate communications centers and unable to effectively communicate with each other.

The San Francisco Fire Department (SFFD) later established an additional "secondary" command post and coordinated its resource requirements back to the SFFD Communications Center using their own radio system. Units that were unable to communicate took actions on their own initiative and were not under the control of the Incident Commander. As one Oakland Fire Department command officer commented "It's hard to get organized and run for your life at the same time!"

The Oakland Hills Fire was the largest response ever recorded. Massive mutual aid was provided by 440 engine companies, 1,539 firefighters and 250 agencies. The equivalent to a 107-alarm fire helped control the inferno. The established mutual aid systems among cities, within counties, and on the regional and statewide levels provided an unprecedented amount of assistance to Oakland and Berkeley for this incident. 88 strike teams were mobilized, some from more than 350 miles away.

The 1991 Oakland disaster was not just a fire problem. Law enforcement, public works and utilities, the National Guard, health and safety services, and relief agencies encountered crushing difficulties. None of these organizations shared a common organizational system or compatible command structure. The Oakland Hills Fire pointed out the need for a common emergency management system throughout local and state government for use by all agencies with a first-responder role associated with public safety.[53]

---

[53] Theodore J. Moody, "Filling the Gap Between NIMS/ICS and the Law Enforcement Initial Response in the Age of the Urban Jihad." (Master's Thesis, Naval Postgraduate School, 2010), http://www.dtic.mil/dtic/tr/fulltext/u2/a531492.pdf.

As a result of the Oakland Hills Fire, a law was passed by the legislature to improve the coordination of state and local emergency response in California. The statute directed OES, in coordination with other state agencies and interested local emergency management agencies, to establish by regulation the Standardized Emergency Management System (SEMS). State agencies and local governments are required to use SEMS to participate in disasters.[54] SEMS required the use of ICS for all public safety agencies in California.

When examining the ICS, research found that Australia has common issues with the United States in wildfires, expanding populations in the urban/wildland interface, and incident management. Australia has similar government emergency response structures where incidents are first handled locally. If incidents expand, mutual aid procedures are utilized, and then state and national resources are applied. Australia had the same needs for an incident management as the United States and utilized the United States ICS as its model.

Australia has had numerous major brushfires in its history. The Black Friday fires of January 1939, in Victoria, Australia, were considered one of the worst natural brushfires in the world, and certainly the single worst in Australian history as a measure of land affected. Almost 20,000 square kilometers (an area about the size of New Jersey) of land was burned and 71 people died.[55]

Significant fires have been a constant since then. The longest official continuous brushfire in New South Wales (NSW) occurred between December 21, 2001, and January 13, 2002. Widespread severe wildfires burned throughout much of NSW during extreme weather conditions.[56] A total of 121 homes were destroyed. Approximately 10,000 people were evacuated and 15,000 firefighters from across Australia and New Zealand

---

[54] "Standardized Emergency Management System," California Code of Regulations, Title 19, Division 2, Chapter 1. Available at http://www.vetmed.ucdavis.edu/vetext/danr/danrguide2_33-38sems.pdf.

[55] "Black Friday - Royal Commission - Judge's Findings - The Fire," ABC News Australia. Available at http://www.abc.net.au/blackfriday/royalcommission/index_findings.htm.

[56] "Attorney-General's Department Disasters Database: Black Christmas Brushfire," Available at. http://www.disasters.ema.gov.au/Browse%20Details/DisasterEventDetails.aspx?DisasterEventID=1320.

were deployed to fight up to 100 large fires for over three weeks, as hot, mainly north-westerly winds and very dry conditions persisted.[57] [58]

Through these and other events, Australia developed the Australasian Inter-Service Incident Management System (AIIMS). The AIIMS is the nationally recognized system of organizational principles and structure used to manage wildfires and other large emergencies (e.g., Floods, Storms and Cyclones etc.) utilizing the *All Agencies* approach.[59] The AIIMS was developed by a committee under the auspices of the then Australian Association of Rural Fire Authorities, since amalgamated into the Australasian Fire Authorities Council in the late 1980s. The system developed by the Australian Association of Rural Fire Authorities was based on the United States National Interagency Incident Management System with modifications to suit the Australian environment. One of the most significant of these was to call the core operational component of the AIIMS, the Incident Control System, in contrast to the United States Incident Command System.[60] This change was to make the terminology used in the AIIMS compliant with existing Australian definitions of command and control. Since command was defined as functioning vertically within organizations and control as functioning horizontally across organizations, the use of control was more appropriate in the Australian context. AIIMS has since been adopted by the various State Emergency Services and a number of other public safety organizations to be the *standard* in Australian emergency response.

As it was developed, AIIMS was an application of Incident Command System, which was claimed to be robust, scalable, and a widely applicable system for dealing with

---

[57] "Attorney-General's Department Disasters Database: Black Christmas Brushfire," Available at. http://www.disasters.ema.gov.au/Browse%20Details/DisasterEventDetails.aspx?DisasterEventID=1320.

[58] "Attorney-General's Department Disasters Database," Available at http://www.em.gov.au/Resources/Pages/DisastersDatabase.aspx.

[59] Julian Yates, "Improving the Management of Emergencies: Enhancing the ICS." *Australian Journal of Emergency Management* 14, no. 2 (Winter 1999): 22–28.

[60] Ibid.

all manner of complex incidents and emergencies.[61] It accomplished this by having various "sectors" "divisions," and "commanders," which can be expanded and contracted dependent on the size of the "emergency." AIIMS was designed to be very similar to the Incident Command System with an Incident Controller, Logistics Section, Operations Section and a Planning Section.

Both the United States and Australian command systems had a Public Information Officer assigned to the command staff and a Communication Unit within the Logistics Section.

4. Oklahoma City Bombing

On April 19, 1995, in Oklahoma City, Oklahoma, terrorism struck when a bomb exploded in front of the Alfred P. Murrah Federal Building. Government and other responders were on the scene minutes after a massive truck bomb destroyed a federal building. The ICS was utilized and one person was appointed as incident commander, responsible for directing all other responders. An after-action report argued that the ''Oklahoma City Bombing should be viewed as ultimate proof that the Incident Command System works."[62] As a result of its perceived success in situations like Oklahoma, the ICS was viewed favorably by the Department of Homeland Security (DHS) for all crisis situations.

5. Federal Adaption

The United States Coast Guard issued Commandant Instruction 3120.1 on September 28, 1998. This instruction directed all Coast Guard units to adopt a standardized response management system for Coast Guard contingency response actions. All officers were to ensure that all personnel involved in response actions are familiar with, and trained in, the use of the National Interagency Incident Management

---

61 "Australasian Fire Authorities Council: Knowledge Web," Available at http://knowledgeweb.afac.com.au/aiims.

62 Oklahoma Department of Civil Emergency Management, "After Action Report :Alfred P. Murrah Federal Building Bombing," n.d.

System (NIIMS)-based ICS. In addition, all contingency plans shall use an ICS structure in their response organization and management procedures.[63]

The September 11, 2001, terrorist attacks highlighted the need to focus on improving emergency management, incident response capabilities, and coordination processes across the country. A comprehensive national approach, applicable at all jurisdictional levels and across functional disciplines, would improve the effectiveness of emergency management/response personnel across the full spectrum of potential incidents and hazard scenarios (including but not limited to natural hazards, terrorist activities, and other manmade disasters). Such an approach was needed to improve coordination and cooperation between public and private agencies/organizations in a variety of emergency management and incident response activities. [64]

To address this deficiency, President Bush issued Homeland Security Presidential Directive (HSPD) 5 in February 2003.[65] The goal of Homeland Security Presidential Directive 5, "Management of Domestic Incidents," was to enhance the ability of the United States to manage domestic incidents by establishing a single, comprehensive national incident management system. HSPD 5 directed the Secretary of the Department of Homeland Security to develop, submit for review to the Homeland Security Council, and administer a National Incident Management System (NIMS). NIMS is to provide a consistent nationwide approach for federal, state, and local governments to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity.

HSPD 5 required all federal departments and agencies to adopt NIMS and to use it in their individual incident management programs and activities, as well as in support of all actions taken to assist state, tribal, and local governments. HSPD 5 mandated that beginning in Fiscal Year 2005, federal departments and agencies shall adopt NIMS. The

---

63 "Commandant Instruction 3120.14," United States Coast Guard. Available at http://www.uscg.mil/directives/ci/3000-3999/ci_3120_14.pdf.

64 Department of Homeland Security. "*National Incident Management System*," 2008, 17.

65 "Homeland Security Presidential Directive 5." February 28, 2003.

directive required federal departments and agencies to make adoption of NIMS by state, tribal, and local organizations a condition for federal preparedness assistance (through grants, contracts, and other activities). The Secretary of the Department of Homeland Security was directed to develop standards and guidelines for determining whether a state or local entity has adopted NIMS.[66]

One of the most important "best practices" that has been incorporated into the NIMS was the ICS. ICS was established by NIMS as the standardized incident organizational structure for the management of all incidents.[67]

6. Katrina

On August 28, 2005, Hurricane Katrina was in the Gulf of Mexico where it powered up to a Category 5 storm on the Saffir-Simpson hurricane scale, packing winds estimated at 175 mph. When Katrina made landfall at 7:10 a.m. on August 29, in southern Plaquemines Parish, Louisiana, it had calmed down to a Category 3 hurricane. Maximum winds were estimated near 125 mph to the east of the center.[68] The storm passed through New Orleans leaving damage in its wake. Tropical storm-force winds and rain extended as far east as the Florida panhandle. A wall of water surged ashore in coastal areas.[69]

Although the storm surge was highest to the east of the path of the eye of Katrina, a very significant storm surge also occurred west of the path of the eye. As the level of Lake Pontchartrain rose, several feet of water were pushed into communities along its northeastern shore in St. Tammany Parish from Slidell to Mandeville, Louisiana. High watermark data indicate the storm surge was 12 to 16 feet in those areas. The surge overtopped large sections of the levees east of New Orleans, in Orleans Parish, and St. Bernard Parish, and it also pushed water up the Intracoastal Waterway and into the

66 "Homeland Security Presidential Directive 5." February 28, 2003.

67 Ibid.

68 "Hurricane Katrina," National Oceanic and Atmospheric Administration. Available at http://www.katrina.noaa.gov/.

69 Ibid.

Industrial Canal. The water rise in Lake Pontchartrain strained the floodwalls along the canals adjacent to its southern shore, including the 17th Street Canal and the London Avenue Canal. Breaches along the Industrial Canal east of downtown New Orleans, the London Avenue Canal north of downtown, and the 17th Street Canal northwest of downtown appear to have occurred during the early morning on August 29. Eventually, about 80 percent of the city of New Orleans flooded, to varying depths up to about 20 feet.[70]

More than 1.5 million people were directly affected and more than 800,000 citizens were forced to live outside of their homes. This was the largest displacement of people since the great Dust Bowl migrations of the 1930s.[71] The total number of fatalities, to be either directly or indirectly related to Katrina, is 1,833. Most of the deaths in Louisiana were directly caused by the widespread storm surge-induced flooding and its miserable aftermath in the New Orleans area.

Hurricanes Katrina and Rita, which hit one month later, were two of the most intense hurricanes ever recorded in the nation's history. The storms had a massive physical impact on the land, affecting 90,000 square miles, an area the size of Great Britain. [72]

Government officials at all levels were unprepared for the consequences of the New Orleans levee breaks. The breaks that inundated the city with floodwater, incapacitated first responders, and stranded the 20 percent of residents who had not evacuated. The breaks pushed the status of Katrina from a bad storm to a catastrophic incident. [73]

The response to Hurricane Katrina did not go well. The Incident Command System was not applied well and not at all in some locations. A coordinated unified

---

[70] "Hurricane Katrina," National Oceanic and Atmospheric Administration. Available at http://www.katrina.noaa.gov/.

[71] "The First Year After Hurricane Katrina: What the Federal Government Did," Department of Homeland Security. n.d. Available at http://www.dhs.gov/xfoia/archives/gc_1157649340100.shtm.

[72] Ibid.

[73] Ibid.

command was not established. Responders were overwhelmed. Local, state, and federal authorities did not understand what was happening and thus did not initially share critical information, quickly organize the response effort, take needed initiative, or work effectively with the media to get the facts to the people.[74] Additional challenges contributed to failed rapid response. Most significant was that policy and law placed the federal government largely in a supplemental role for natural disasters. Federal law (the Constitution, Stafford Act, and Insurrection Act) put state leadership at the center of incident management and tied federal response to specific state requests. The overall relief effort was framed by the National Response Plan (NRP), which called for a sequential reaction: local, then state, then federal.[75]

7. Deepwater Horizon

On the evening of April 20, 2010, a gas release and subsequent explosion occurred on the Deepwater Horizon oil rig working on the Macondo exploration well for BP southeast of Venice, Louisiana, in the Gulf of Mexico. The fire burned for 36 hours before the rig sank, and hydrocarbons leaked into the Gulf of Mexico for 87 days before the well was closed and sealed.76

On April 23, the Coast Guard established a robust Incident Command System response in accordance with the National Oil and Hazardous Substances Pollution Contingency Plan (NCP). The ICS provided a common command and control framework to develop and implement tactical plans to effectively manage a multi-agency response to emergencies. The ICS organization for this response included Incident Command Posts and Unified Commands at the local level and a Unified Area Command at the regional

---

74 Gregory A. S. Gecowets, and Jefferson P. Marquis "Applying the Lessons of Katrina," *Joint Forces Quarterly* Issue 48, 1st quarter 2008. *Available at* http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA518742. 70–76.

75 Ibid.

76 "Deepwater Horizon" National Oceanic and Atmospheric Administration. Available at http://www.noaa.gov/deepwaterhorizon/.

level, and consisted of representatives from the Coast Guard, other federal, state, and local agencies, as well as BP as the primary responsible party.[77]

Overall, the incident command structure functioned appropriately; however, with an incident spreading across hundreds of miles of coastline, issues occurred.

In testimony, Craig Paul Taffaro Jr. stated that of significant importance was the clear indication that the response to the Deepwater Horizon Oil Spill crisis started from a position of playing catch up. From the breaking notice that an explosion had occurred many weeks later, the information flow to the local branch was wrought with inconsistency, fragmented messaging, and stove-piped communication patterns. He stated that for the first six weeks of the response, despite an approved joint command and incident command team being built, a separate and uncoordinated effort was the norm.[78]

This lack of continuity was addressed by the local community by establishing a deputy lead in all ICS sections, which was also attempted to be undone at various times throughout the rotation of BP and Coast Guard personnel. As branch directors, deputies, PPLOs, and other subject matter experts from the Coast Guard and/or BP contractors rotated into the St. Bernard Parish Branch, a constant learning curve was experienced, and a re-tooling of operational, logistical, planning, and resourcing activities became the norm. This contention often was the result of an Incident Command in Houma not recognizing the operational input and planning of the local branch in St. Bernard Parish.[79]

Taffaro stated:

> We recognize that a basic tenet of disaster response is that disasters are local. To exclude local engagement curtails critical information and hinders the process of an expedited response. While following a National Contingency Plan may set the specific command parameters and structure,

---

[77] Committee on Homeland Security: Hearings on Preliminary the Lessons from Deepwater Horizon. 111th Cong. (2010). September 22, 2010. Serial No. 111–80. Statement of Mr. Craig Paul Taffaro, Jr., St. Bernard Parish, Louisiana.

[78] Ibid., 19.

[79] Ibid., 20.

> if implemented without local buy-in initiates significant but unnecessary power struggles, stifles valuable information exchange, breeds distrust, and ultimately interferes with the effective completion of the mission at hand via distractions which focus on personality and authority dynamics.[80]

Rear Admiral Peter Neffenger, Deputy National Incident Commander for the Deepwater Horizon incident, stated that the Deepwater Horizon event displayed that work is needed with all the agencies to review the National Contingency Plan and the National Response Framework to identify national-level issues to enhance our ability to provide a coordinated, whole of government response to major incidents.[81]

The ICS has grown, evolved, and matured from the early days when FIRESCOPE was formed. The ICS has changed to include an all-risk environment that all agencies can use. Through that evolution, ICS has spread from Southern California, to the State of California, and then throughout the Nation. ICS will continue to change to meet the challenges of the ever-evolving threat environment. The events of Katrina and Deepwater Horizon have shown that the Incident Command System needs further work to ensure that it can work efficiently and effectively for the betterment of the citizens it is intended to protect. The following chapter explores the literature of the ICS.

---

[80] Committee on Homeland Security: Hearings on Preliminary the Lessons from Deepwater Horizon. 111th Cong. (2010). September 22, 2010. Serial No. 111–80. Statement of Mr. Craig Paul Taffaro, Jr., St. Bernard Parish, Louisiana. 19.

[81] Ibid., 30.

THIS PAGE INTENTIONALLY LEFT BLANK

III. LITERATURE REVIEW

It's hard to get organized and run for your life at the same time!

Oakland Fire Department command officer at Oakland Hills Fire

A. INTRODUCTION

Literature pertaining to the topics being explored in this thesis falls into three primary categories. First, there is the literature that the federal government has published identifying and describing the Incident Command System. Much of this literature has appeared in the wake of the September 11 attacks against civilian targets in the cities of New York, Washington, and Somerset County, Pennsylvania. This body of recent work describes the ICS and outlines the mandatory shift in emergency management protocols.

Second, there is the body of literature that describes the growth and maturation of the ICS. This literature discusses and debates some of the questions about the ICS that will resurface in later years. Some of these topics have not had sufficient discourse. This is the body of literature that questions the applicability of ICS to the range of crisis responses. This literature made its appearance relatively quickly following the development of ICS in California in the 1970s, but developed more during the 1990s. Its emphasis is sector-based, in that its core assertion challenges the effectiveness of NIMS/ ICS for all type of emergency incidents.

Third, there is a scholarly body of literature, drawing on the work of the Disaster Research Center. In it, Arnold Howett, Dutch Leonard, and others question the ability of NIMS/ ICS to function equally well across all emergent situations, across the response spectrum. This literature is important to our discussion because NIMS and ICS was established, by the federal government, as the singular solution to crisis management in the decade since September 11, 2001.

1. Federal Literature

Integration of ICS as the national model for emergency management was initiated in February, 2003, when President Bush issued Homeland Security Presidential Directive (HSPD) 5. The goal of HSPD 5 "Management of Domestic Incidents," was to enhance the ability of the United States to manage domestic incidents by establishing a single, comprehensive national incident management system. HSPD 5 directed the Secretary of the Department of Homeland Security to develop, submit for review to the Homeland Security Council, and administer a National Incident Management System (NIMS). NIMS is to provide a consistent nationwide approach for federal, state, and local governments to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity.[82] HSPD 5 required all federal departments and agencies to adopt NIMS and to use it in their individual incident management programs and activities, as well as in support of all actions taken to assist state, tribal, and local governments. HSPD 5 mandated that beginning in Fiscal Year 2005, federal departments and agencies shall adopt NIMS.

Following HSPD 5, the Department of Homeland Security released the NIMS on March 1, 2004.[83] The NIMS describes the ICS and its component parts. NIMS incorporated the best practices currently in use by the emergency response community. In the introductory letter signed by Tom Ridge, the first Secretary of the Department of Homeland Security states that NIMS had undergone extensive vetting within the federal family and also included a development process with extensive outreach to state, local and tribal officials, to the emergency response community, and to private officials.[84]

The federal government had already been using the ICS within some departments. The United States Forest Service approved implementation of ICS in the Pacific

82 "Homeland Security Presidential Directive 5," February 28, 2003.

83 Department of Homeland Security, "*National Incident Management System*." 2004.

84 Ibid., 5.

Southwest Region by 1983, and implemented it service wide by 1985.[85] In 1989, the Federal Emergency Management Agency (FEMA) established the National Urban Search and Rescue (US&R) Response System as a framework for combining local emergency services personnel into integrated disaster response task forces. These task forces, designated as federal resources, were to be deployed through the Response Directorate of FEMA. The task forces were the primary response asset at FEMA.[86] The task forces, developed primarily from fire departments around the nation, brought their ICS with them and integrated it into the federal response. In 1992, the federal government accepted ICS as the incident management system with the adaption of the Federal Response Plan.[87] The Federal Response Plan described the structure for organizing, coordination, and mobilizing federal resources to augment state and local response efforts under the Stafford Act. The ICS was identified as the structure for integrating those federal resources.

A key component of NIMS is the outline of the NIMS National Integration Center. The National Integration Center is responsible for facilitating the development and adoption of national-level standards, guidelines, and protocols related to the NIMS.[88] The National Integration Center provides strategic direction for and oversight of NIMS and continuous refinement of the system and its components over the long term. Revisions to NIMS, ICS and other issues can be proposed by any and all NIMS users.

Accompanying the NIMS, was the National Response Plan (NRP).[89] The NRP was to address activities related to domestic incident management, including prevention, preparedness, response, and recovery actions. The NRP focused on those activities that

---

85 "Some Highlights of the Evolution of the Incident Command System," Available at http://www.firescope.org/firescope-history/Some%20Highlights%20of%20the%20Evolution%20of%20the%20ICS.pdf.

86 "Urban Search and Rescue (US&R)," Federal Emergency Management Agency. Available at http://www.fema.gov/emergency/usr/.

87 "Federal Response Plan," *Public Law 93-288 as Amended 1992*, n.d. Available at http://library.findlaw.com/1992/Apr/1/127810.html.

88 Department of Homeland Security, "National Response Plan," 2004. Available at http://www.it.ojp.gov/fusioncenterguidelines/NRPbaseplan.pdf," 77.

89 Ibid.

are directly related to an evolving incident or potential incident. The NRP broke new ground in integrating all levels of government in a common incident management framework.

Due to issues raised after the response to Hurricane Katrina and the hurricane season of 2005, the National Response Plan was updated and recreated as the National Response Framework (NRF) in 2008.[90] Changes were made to the NRP that were both structural and significant. The Department of Homeland Security was advised that NRP were bureaucratic and repetitive. Users also suggested the NRP was still insufficiently national in its focus, which is to say that it should speak more clearly to the roles and responsibilities of all parties involved in response. Clearly, it was evident that the NRP and its supporting documents did not constitute a true operational plan in the sense understood by emergency managers. The National Response Plan did not live up to the promise of its title.

The NRF was intended to be a more of a framework to guide the effective response to an incident is a shared responsibility of governments at all levels, the private sector and non-governmental organizations (NGOs), and individual citizens. The NRF took the experience gained since the 1992 Federal Response Plan (FRP) through the 2004 NRP combined with intervening incidents to create a more mature plan for all incidents.

With the NRF came numerous other documents, like the updated NIMS[91] and National Incident Management System: Five-Year NIMS Training Plan.[92] Together, these documents describe to foundation of incident management and ICS.

---

[90] Department of Homeland Security, "National Response Framework," 2008. Available at http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf

[91] Department of Homeland Security. "*National Incident Management System*," 2008

[92] National Integration Center (NIC), Incident Management Systems Integration Division. "National Incident Management System (NIMS): Five-Year NIMS Training Plan," 2008. Available at http://www.nema.ne.gov/pdf/fy08-nims-5yearplan.pdf.

2. Growth and Maturation of the ICS

The ICS grew out of necessity, due to a series of incidents in the 1970s, and was primarily developed to handle the large fires in the west. It represented a significant departure from previous large-scale emergency coordination methods where ad hoc networks were put together and had to work through their differences on-site.[93] By 1978, parts of the ICS were successfully used on several wildland fire incidents and applied to urban firefighting. That year, ICS was formally adopted by the Los Angeles Fire Department as the incident management structure for all incidents.[94] ICS soon spread across the fire service and through the fire service's response spectrum.

Additional command and control systems were developed over the years, including the Fireground Command System (FGC) developed by the Phoenix, Arizona Fire Department and the National Fire Service Incident Management System.[95] The concepts of FGC were similar to ICS, although there were differences in terminology and in organizational structure. The FGC system was developed for structural firefighting and was designed for operations of 25 or fewer companies.[96]

Recognizing the continuing challenges occurring in the fire service in applying a common approach to incident command, the National Fire Service Incident Management System (IMS) Consortium was created in 1990. Its purpose was to create consensus towards developing a single command system. The consortium consisted of many individual fire service leaders, representatives of most major fire service organizations and representatives of federal, state and local agencies, including FIRESCOPE and the Phoenix Fire Department. One of the significant outcomes of the consortium's work was an agreement on the need to develop operational protocols within ICS, so that responders

---

93 "History of ICS." National Wildland Coordinating Group, National Training Curriculum, October 1994. Available at http://www.nwcg.gov/pms/forms/compan/history.pdf.

94 Ibid.

95 "National Incident Management System Consortium", Available at http://www.ims-consortium.org/backinfo.htm.

96 Duane M. Smith, "A Study of Command And Control of Multi-Agency Disaster Response Operations." (Doctoral Thesis, University of Phoenix, December 2010) Available at http://pqdtopen.proquest.com/#viewpdf?dispub=3467495.

would be able to apply the ICS as one common system. In 1993, the IMS consortium completed its first document: Model Procedures Guide for Structural Firefighting.[97] The National Fire Academy, having already adopted the ICS in 1980, incorporated this material into its training curriculum as well.

The 911 Commission report was very clear about the direction the nation should take when is recommended that emergency response agencies nationwide should adopt the Incident Command System.[98] The report gives credit to the ICS at the Pentagon response. It states that the emergency response at the Pentagon represented a mix of local, state, and federal jurisdictions and was generally effective. It overcame the inherent complications of a response across jurisdictions because of the Incident Command System.[99]

However, a point that the 911 Commission brought up was communication. It stated that the inability to communicate was a critical element at the World Trade Center, Pentagon, and Somerset County, Pennsylvania, crash sites, where multiple agencies and multiple jurisdictions responded. The occurrence of this problem at three very different sites is strong evidence that compatible and adequate communications among public safety organizations at the local, state, and federal levels remains an important problem.[100] Communication is a function the ICS; communication failure could be an inherent fault of the system and should be a point of further debate.

3. Scholarly Literature

Wenger et al**.** asked in 1989 if the Incident Command System is the ideal model for all emergency management.[101] They identified serious difficulties in the ICS. First

---

97 "Unit 7 - Fireground Command," John Jay College of Criminal Justice. Available at. http://web.jjay.cuny.edu/~tflan/documents/101docs/FIS101FiregroundCommand.pdf.

98 "*9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*." New York: W. W. Norton & Company, 2004. 415.

99 Ibid., 332.

100 Ibid., 415.

101 Dennis Wenger, E. L. Quarantelli, Russell R Dynes, "Disaster Analysis: Police and Fire Departments." *Disaster Research Center*, 1989.

was the concept that ICS had become a buzzword within emergency management that bears little relationship to the detailed management model. Many departments claim to use the ICS, however, during actual emergencies; the plan is either ignored or is utilized in a very limited fashion. Furthermore, while many departments have some knowledge of the concepts, few understand the complexities and purposes of the system. Another issue they have with ICS is communications. Case studies indicated that communication systems failed due to overload. Communication between units, and command posts and communication centers, were lost.[102] They state that before jumping on the ICS "bandwagon," careful, critical analysis of the model must be undertaken. It should be adapted and implemented with care.[103] These arguments were well grounded at the time. However, in 1989, ICS was in its infancy and many organizations were new to the system or were only beginning the transition. These criticisms may seem premature. Wenger et al., stated that ICS is far from perfect. They continued that, as is the case with any rapidly growing technology, the adoption of ICS by new user groups is rarely painless or seamless. For example, few fire departments have escaped the "growing pains" that inevitably accompany the initial integration of ICS into traditional operational environments.[104]

Research displayed a dearth of critical examinations of the issues raised by Wenger et al. Outside of the fire service, little research on the ICS was completed. Prior to 1989, literature on police activity during community emergencies and disasters was very limited.[105]

In 1998, Quarantelli again critiqued ICS and described the widespread adaption of the ICS as "a fad." He stated that ICS use, pushed by the fire service, as an organization/operational model for disaster management had not been supported with

---

[102] Dennis Wenger, E. L. Quarantelli, and Russell R Dynes, "Disaster Analysis: Police and Fire Departments." *Disaster Research Center*, 1989.

[103] Ibid., 164.

[104] Dennis Wenger, E. L. Quarantelli, and Russell R Dynes, "Is the Incident Command System a Plan for All Seasons and Emergency Solutions." *Hazard Monthly*, May 1990."

[105] Dennis Wenger, E. L. Quarantelli, and Russell R Dynes, "Disaster Analysis: Police and Fire Departments." *Disaster Research Center*, 1989.

empirical evidence and may not be a good idea.[106]. Federal literature does not address the concerns of Quarantelli. ICS had gained momentum and serious debate was limited. The greatest strength of the Incident Command System is that it's widely known; its greatest weakness is that ICS is not widely understood.[107]

For the fire service, ICS was a creative, even necessary, managerial invention that addressed core professional problems. It made good sense to train and exercise all personnel in the system and use it regularly even when responding to small events. ICS became virtually second nature when emergent crises made it essential.

Howitt and Leonard declared that for law enforcement in the U.S., the need for ICS was less certain. Comparing policing to firefighting, they noted that active field co-ordination involving significant numbers of officers occurs much less regularly (though it does occur, for example, in security for large events, hostage situations, and drug arrests). Collaboration with mutual aid providers from other jurisdictions is quite rare. Howitt and Leonard continue that law enforcement's need for ICS may seem less compelling than the fire service, and the costs of preparing personnel and the organization as a whole may seem more burdensome, perhaps unjustified. They continue that, other response professions, particularly public health and hospital-based emergency medicine, may for varying reasons, find it difficult to identify the key operational questions for which ICS is the answer.[108] Moody states that the NIMS-based model alone, when considering the current *National Response Scenarios*, seems ill suited for response to acts of paramilitary terrorism. American law enforcement may require a supplemental response paradigm that envisions an effective initial response when faced with degraded communications

---

106 E. L.Quarantelli, "Disaster Planning, Emergency Management, and Civil Protection: The Historical Development and Current Characteristics of Organized Efforts to Prevent and to Respond to Disasters.' *Disaster Research Center*, 1998."

107 Bill Sager, "Command Confusion," *Wildfire Magazine*. Available online at http://wildfiremag.com/command/command_confusion/.

108 Arnold M. Howitt and Herman B. Leonard, "A Command System for All Agencies?" *Crisis/Response Journal*, March 2005, 40–42.

capabilities and uncertain command and control structures.[109] NIMS and ICS are important tools that can be adapted to establish command and control in coordinating aspects of the response and recovery phases of many major incidents, including some types of terrorist attacks. Moody questions that these command and control paradigms, however, are heavily reliant on communications technology and other social and organizational preconditions, and may fail to adequately support the initial law enforcement response to some types of incidents, such as the attacks that occurred in Mumbai, India and Lahore, Pakistan.[110]

The National Incident Management System Consortium states that since the establishment of the NIMS by the Homeland Security Department, law enforcement agencies across the nation have diligently made efforts to comply with the spirit, intention and letter of the directives. Efforts to develop congruence with NIMS include the incorporation of the principles of the ICS into basic police academy curriculum, integration into daily activities, and special operations across the nation.[111]

However, Howett also describes ICS as a proven versatile incident management tool that is effective in diverse settings.[112] He stated that "from the birthplace of ICS in California to the National Fire Academy and FEMA, the consensus among long-time practitioners seems to be that ICS works."[113] However, as Katrina revealed, basic

---

109 Theodore J. Moody, "Filling The Gap Between Nims/Ics and the Law Enforcement Initial Response in the Age of the Urban Jihad." Master's Thesis, Naval Postgraduate School, 2010), http://www.dtic.mil/dtic/tr/fulltext/u2/a531492.pdf.

110 Ibid., 2.

111 David Matthew and Thomas A Maloney, "The Application of the National Incident Management System In Law Enforcement Operations," National Incident Management System Consortium. July 2009. Available at http://www.ims-consortium.org/NIMSC_White_Paper_Final_Version.pdf.

112 Arnold M Howitt and Herman B Leonard, "A Command System for All Agencies?" *Crisis/Response Journal*, March 2005, 40–42.

113 Dana Cole, "The Incident Command System: A 25-Year Evaluation by California Practitioners." *National Fire Academy*, February 2000. Available at http://www.hsdl.org/?view&doc=45746&coll=limited. 7.

diffusion of ICS and NIMS has not been completed in many jurisdictions. Many have not previously used the system, and many professional disciplines have been unaware or unenthusiastic.[114]

Buck et al. raise concerns expressed that ICS has limitations in serving as a model for disaster response.[115] Research has identified various limitations in the ICS's model serving for all hazards. These limitations include the following: (a) network governance, (b) integrating conduct of multiple response organizations, (c) and integrating on nongovernmental agencies. They continue that the inability of ICS to accommodate easily the inclusion of nongovernment agencies, whether they are private corporations or nonprofit entities, is a continuing weakness that has not been satisfactorily addressed since the ICS system was implemented. The potential limitations of the ICS as a command and control system are further identified by Buck et al., who observed that "ICS, as is true for all rational forms of organization, only works when a series of preconditions are met."[116]

Buck et al. expressed concern for ICS's lack of focus on coordination between organizations and levels of government responding to disaster. The debate has gained importance since the federal government's mandate to make ICS the disaster operations standard. They assert that ICS is flawed and that ICS usage may exacerbate the difficulties in the organization of emergency response.[117]

Since NIMS and ICS had been adopted by numerous federal agencies including FEMA, the Forest Service, and the Coast Guard,[118] little discussion or criticism emerged

---

114 Arnold M Howitt and Herman B Leonard, "A Command System for All Agencies?" *Crisis/Response Journal*, March 2005, 40–42.

115 Dick A Buck, Joseph E Trainor, and Benigno E Aguirre, "A Critical Evaluation of the Incident Command System and NIMS." *Journal of Homeland Security and Emergency Management* , no. 3 (2006). Available at http://www.bepress.com/jhsem/vol3/iss3/1.

116 Ibid., 11.

117 Dick A Buck, Joseph E Trainor, and Benigno E Aguirre, "A Critical Evaluation of the Incident Command System and NIMS." *Journal of Homeland Security and Emergency Management*, no. 3 (2006). Available at http://www.bepress.com/jhsem/vol3/iss3/1.

118 Commandant Instruction 3120.14, United States Coast Guard. Available at http://www.uscg.mil/directives/ci/3000-3999/ci_3120_14.pdf.

arguing the benefits or detractions individual components of the system. The federal government assumed that ICS was an all-or-nothing proposal and no alternatives were discussed. However, there are alternatives. The Incident Command System is based upon five basic functions: command, operations, planning, logistics and finance. However, little discussion enters into the discourse, if these are the only basic functions. It can be argued that the demands for public information in large-scale emergencies has become so demanding that public information should be a discrete function in its own right. The United Kingdom's Gold, Silver, Bronze system is another example of incident management that should enter into the debate.[119]

The current ICS has communications as a sub-function of logistics. That may not be the most appropriate place or level of function within the ICS. As stated, the 911 Report lists communication as a fault with the Pentagon response. Would elevating communication to a basic function reduce issues? The Australian ICS is very similar to the United States version. It lists communication among the basic functions.[120] Australia also lists public information in as a basic function. Due to fires in 2009, Australia raised the function of public information to a separate section reporting directly to the incident commander.

Discussions about the ICS have been mixed. Parts of the response community offer praise, while others are critical of ICS. To paraphrase Winston Churchill's comments on democracy, it has been said that the Incident Command System is the worst form of incident management except all the others that have been tried. However, that does not mean we stop debating and attempting to improve on the system. ICS works well when official responders have trained in ICS and have a strong sense of community. However, the case is not closed on how the system can be improved. The next chapter defines the identified communication problems in more detail and research methodology with the intent of creating a stronger system.

---

119 "Major Incident Procedure Manual," London Emergency Services Liaison Panel. TSO (The Stationery Office), 2007. Available at www.tsoshop.co.uk.

120 Julian Yates, "Improving the Management of Emergencies: Enhancing the ICS." *Australian Journal of Emergency Management* 14, no. 2 (Winter 1999): 22–28.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. DEFINITION OF THE PROBLEM—COMMUNICATIONS FAILURES IN THE ICS

A. INTRODUCTION

This chapter further defines the problem and discusses the research questions. In addition, Chapter IV explores the research methodology, Soft Systems Methodology (SSM). SSM is designed to shape interventions in the problematic situations encountered in complex organizational contexts, where there are often no easily identified solutions. Though aligned with systems engineering approaches, it breaks with them by recognizing the central importance of perspective or world-view in social situations.[121]

Information is the most valuable commodity during emergencies or disasters. It is what everyone needs to make decisions. It is an essential aspect in an organization's ability to gain (or lose) command and control, visibility, and credibility. Above all, it is necessary for rapid and effective assistance for those affected by a disaster. [122]

As stated in the NIMS documents,

> Effective emergency management and incident response activities rely on effective, flexible communications and information systems that provide information and a common operating picture to emergency management, response personnel and the public. Communications properly planned, established, and applied enable the dissemination of information among command and support elements and, as appropriate, cooperating agencies and organizations.[123]

---

121 Stan Lester, "*Soft System Methodology*," April 2008. Available at http://www.sld.demon.co.uk/ssm.pdf,

122 S. A. Barrantes, M RodrIguez, and R Pérez, "*Information Management and Communication in Emergencies and Disasters*." Pan American Health Organization, 2009. Available at http://www.allindiary.org/pool/resources/4-2-im-commguide-responseteams-paho-2009.pdf.

123 Department of Homeland Security, "*National Incident Management System*," 2008. 23.

Successful communications and information management require that emergency management and response personnel use standardized communications types. NIMS describe these types as:

- ***Strategic Communications:*** High-level directions, including resource priority decisions, roles and responsibilities determinations, and overall incident response courses of action.
- ***Tactical Communications:*** Communications between command and support elements and, as appropriate, cooperating agencies and organizations.
- ***Support Communications:*** Coordination in support of strategic and tactical communications (for example, communications among hospitals concerning resource ordering, dispatching, and tracking from logistics centers; traffic and public works communications).
- ***Public Address Communications:*** Emergency alerts and warnings, press conferences, etc.[124]

Strategic, tactical and support communications are facilitated through the Communications Unit within the Incident Command System.

1. Internal Communications

The Logistics Section provides for all the support needs for the incident, such as ordering resources and providing facilities, transportation, supplies, equipment maintenance and fuel, food service, communications, and medical services for incident personnel. The Logistics Section is led by a Section Chief, who may also have one or more deputies. Having a deputy is encouraged when all designated units are established at an incident site. When the incident is very large or requires a number of facilities with large numbers of equipment, the Logistics Section can be divided into branches. This helps with span of control by providing more effective supervision and coordination among the individual units.

[124] Department of Homeland Security, "*National Incident Management System*," 2008. 25.

The Communications Unit reports to the Logistics Section Chief and develops the Communications Plan to make the most effective use of the communications equipment and facilities assigned to the incident. Additionally, this unit installs and tests all communications equipment, supervises and operates the incident communications center, distributes and recovers communications equipment assigned to incident personnel, and maintains and repairs communications equipment on site.

Internal communications are facilitated through the development and use of common communications plans and interoperable communications equipment, processes, standards, and architectures. During an incident, this integrated approach links the operational and support units of the various organizations to maintain communications connectivity and situational awareness. Establishing and maintaining a common operating picture and ensuring accessibility and interoperability are the principal goals of the Communications and Information Management component of NIMS.[125] Properly planned, established, and applied communications enable the dissemination of information among command and support elements and, as appropriate, cooperating agencies and organizations.

The Communications Unit is responsible for effective incident communications planning, especially in the context of a multiagency incident. All communications between organizational elements during an incident should be in plain language (clear text) to ensure that information dissemination is clear and understood by all intended recipients. Communications planning is critical for determining required radio networks, establishing interagency frequency assignments, and ensuring the interoperability and the optimal use of all assigned communications capabilities.

The Communications Unit Leader should attend all Incident Planning Meetings to ensure that the communication systems available for the incident can support the tactical operations planned for the next operational period and beyond. Advance planning is required to ensure that appropriate communications systems are available to support

[125] Department of Homeland Security, "*National Incident Management System*," 2008. 23.

incident operations requirements. This planning includes the development of frequency inventories, frequency-use agreements, and interagency radio caches.

Most complex incidents will require a Communications Plan (ICS 205). The Communications Unit is responsible for planning the use of radio frequencies; establishing networks for command, tactical, support, and air units; setting up on-scene telephone and public address equipment; and providing any required off-incident communication links. In addition, the Communication Unit should establish computer networks to facilitate Internet and email.[126] Newer technologies, including global position system (GPS) devices and voice over IP (VOIP) must be included in current and future Communications Unit considerations.

Radio networks for large incidents may be organized as follows:

1. **Command Net:** The command net links together Incident Command, Command Staff, Section Chiefs, Branch Directors, and Division and Group Supervisors.

2. **Tactical Nets:** Several tactical nets may be established to connect departments, agencies, geographical areas, or specific functional units. The determination of how nets are set up should be a joint function designed by Planning, Operations, and Logistics.

3. **Support Net:** A support net may be established primarily to handle changes in resource status but also to handle logistical requests and other non-tactical functions.

4. **Air-to-Ground Net:** To coordinate air-to-ground traffic, either a specific tactical frequency may be designated, or regular tactical nets may be used.

5. **Air-to-Air Nets:** Air-to-air nets may be designated and assigned for use at the incident. An air-to-air net is designed to be used by airborne assets; ground units should not utilize this net.[127]

A better approach has been suggested. Rather than focus on mission effectiveness, which requires a specific scenario, it has been suggested that one focus instead on agility.

---

126 Department of Homeland Security, "*National Incident Management System*," 2008. 89.

127 Ibid., 109.

Agility is the ability to successfully cope with a variety of circumstances and stresses. Threats to successfully coping can come from a variety of sources. The six components of agility are: 1) robustness, 2) flexibility, 3) responsiveness, 4) resilience, 5) adaptability, and 6) innovation. [128]

2. External Communications

The Public Information Officer is responsible for interfacing with the public and media and/or with other agencies with incident-related information requirements. The Public Information Officer is part of the incident Command Staff and as such assistants may be assigned, including assistants from other involved agencies, departments, or organizations. The Public Information Officer gathers, verifies, coordinates, and disseminates accurate, accessible, and timely information on the incident's cause, size, and current situation; resources committed; and other matters of general interest for both internal and external audiences. The Public Information Officer may also perform a key public information-monitoring role. Whether the command structure is single or unified, only one Public Information Officer should be designated per incident. The IC/UC must approve the release of all incident-related information. In large-scale incidents or where multiple command posts are established, the Public Information Officer should participate in or lead the Joint Information Center (JIC) in order to ensure consistency in the provision of information to the public.[129]

The Public Information Officer advises the IC/UC on all public information matters relating to the management of the incident. The Public Information Officer also handles inquiries from the media, the public, and elected officials; emergency public information and warnings; rumor monitoring and response; media relations; and other

---

[128] David S Alberts and Richard E Hayes, "*Power and Control: Command and Control in the Information Age*," Available at http://www.dodccrp.org/files/Alberts_Power.pdf.

[129] Department of Homeland Security. "*National Incident Management System*," 2008. 92.

functions required to gather, verify, coordinate, and disseminate accurate, accessible, and timely information related to the incident. Information on public health, safety, and protection is of particular importance.[130]

3. Problem Statement

The problem is that the ICS is not meeting the current needs of the citizens. Responders describe the situation after a March 2000 tornado in Fort Worth, Texas: Problems evident during the response was a lack of initial communication between field personnel and emergency managers in the operations center. After the tornado dissipated, the emergency operations center (EOC) sent city crews into the downtown area to start the process of debris removal. Unfortunately, the emergency operations center was not aware of the dangerous condition owing to the hanging glass from the high-rise buildings.[131]

In events of national significance since its adoption in 2004, inter-incident communications have not performed, causing numerous response problems. As more accounts of decision making during Katrina become part of the public record, it becomes apparent that major shortcomings of situational awareness resulted because information about conditions was unavailable and/or did not reach senior decision makers.

In multiple reports from the National Institute for Occupational Health and Safety (NIOSH) fire-fatality reports to after action reports of large, complex incidents, communication issues continue to be identified.

In addition, external communications or public information systems have failed to meet the community's expectations and keep the public informed about the size, scope, and impact of the emergency. As stated in Congressional hearings regarding the Deepwater Horizon spill, the flow of information was poor. Craig Paul Taffaro Jr., president of St. Bernard Parish, stated, "The information presented by BP in print and

---

130 Department of Homeland Security. "*National Incident Management System*," 2008. 70.

131 Patrick C. Smith and David M. Simpson, "The Role of Mobile Emergency Tactical Communication Systems for Disaster Response," 2005. Available at http://hazardcenter.louisville.edu/pdfs/wp0605.pdf.

broadcast media often erupted into episodes of frustration and disbelief as disconnect between the reality of a local experience and the stated information was clearly displayed."[132] The challenge to share information was never conquered.

The main challenge of external communications or public information systems is to ensure that information is clear and that it reflects the most urgent needs of the affected population. The second major challenge is to produce and update information regularly. Moreover, public and social communication and media relations have become key elements in efficient emergency management. Technical operations in highly charged emergency situations must be accompanied by good public communication and information strategies that take all stakeholders into account.

Twenty-first century challenges, increasingly complex incidents, and the continued maturation of networking (e.g., social, communications, information) concepts, technologies, and services combined have to create a schism between the ways in which ICS was and, for the most part, still is conceptualized, studied, and practiced, and what is required for success.

Since the creation of the ICS, society and society's expectations of incident management have changed. This disconnect is not limited to incident management. Networking capabilities have not only fundamentally changed the economics of information, but they have also changed the way individuals and organizations relate to one another throughout society. The ICS was developed in the 1970s and, since then, has undergone few changes or modifications.

The failures of the incident management system create increased impact from hurricanes, fires, floods, and other emergency incidents by reducing the efficiency of the management system. In addition, the public is increasingly uninformed as to the incident, their expected actions, and threats to public safety. The ultimate effect is that the public is adversely impacted due to the emergency management's deficiencies.

---

[132] Committee on Homeland Security: Hearings on Preliminary the Lessons from Deepwater Horizon. 111th Cong. (2010). September 22, 2010. Serial No. 111–80. Statement of Mr. Craig Paul Taffaro, Jr., St. Bernard Parish, Louisiana.

The multiple incidents have served to illustrate that timely communication is vital in an emergency and the availability of critical information can help individuals protect themselves from harm. Be it through television, radio, mobile devices, the Internet, social media, reverse 911, or warning sirens, emergency managers and emergency response providers must have prompt and reliable means to provide information to their citizens.[133]

Effective communication and information management are obviously critical to the overall process of managing and reducing the risks of disaster.

The problem centers on the ICS and implementation. Specifically, the scope of the problem is to focus on incident communications, including internal and external communications (public information). The problem is that internal communication policies, procedures, and systems have failed to keep leaders informed of the size and scope of the emergencies. This has led to poor decision making by incident commanders and other response problems. Also, internal communication systems have not expanded to include the information systems to supplement or supplant voice radio systems. In addition, public information (external communications) has failed to keep the citizens informed about the size, scope and impact of the emergency. Advances in information technologies have created a new space within which individuals and organizations can operate. Those individuals and organizations that have learned to take advantage of the opportunities afforded by operating in this new space have realized a significant advantage over those that have ignored these opportunities.

4. Research Questions

In order to assess the problem, the research methodology addresses the following research questions:

1. Which type of structure would make communications in the ICS more efficient?

[133] Committee on Homeland Security, Subcommittee on Emergency Preparedness, Response, and Communications. Hearings on Communicating with the Public During Emergencies, 112th Cong. (2010) July 8, 2011**.** Available At Https://Www.Hsdl.Org/?View&Did=489262.

2. Are internal (incident communications) and external communications (public information) related sufficiently so that they can be combined within the ICS?

3. Or, do internal and external communications need to remain separated to operate efficiently?

4. Would the changing the ICS communications structure meet the community's current expectations?

5. What are the externalities that would prevent implementation of any recommended changes to the ICS?

5. Research Methodology

In order to fully discuss and answer the research questions, a Soft systems methodology was utilized. Soft Systems Methodology (SSM) is the result of the continuing action research that Peter Checkland, Brian Wilson, and many others have conducted over 30 years, to provide a framework for users to deal with the kind of messy problem situations that lack a formal problem definition. The theme of SSM is taking purposeful action in human situations regarded as problematical. It is an organized process of inquiry, based on systems models, which leads to choice of purposeful action. It is built around the concept of the human activity system.[134]

The original version of SSM as a seven-stage methodology published in Checkland's "Systems Thinking, Systems Practice"[135] has since been superseded in Checkland's work. The seven-stage model was utilized in this research. The seven stages are:

1. Entering the problem situation.

2. Expressing the problem situation.

3. Formulating root definitions of relevant systems.

---

134 Peter Checkland, "Achieving 'Desirable and Feasible' Change: An Application of Soft Systems Methodology," *Journal of the Operational Research Society.* Vol 6, No 9, 1985. 821-831 Available at http://www.palgrave-journals.com/jors/journal/v36/n9/pdf/jors1985148a.pdf.

135 Peter Checkland, *Systems Thinking, Systems Practice*. New Jersey: John Wiley & Sons, 1999.

4. Building Conceptual Models of Human Activity Systems.

5. Comparing the models with the real world.

6. Defining changes that are desirable and feasible.

7. Taking action to improve the real world situation.

Realizing steps (1) and (2) have been completed with the problem statement and research questions, this methodology would fit well within the structure of this paper. In addition, the root definitions of relevant internal and external communication systems within the ICS (3) have been discussed. This model then forms the basis for real-world changes.[136]

The selection of the SSM was made to assist in the formation of solutions to the research questions and problems identified, and to evaluate possible solutions. Through the SSM, assessment and of alternative courses of possible action will be explored. The assessment will include changing incident management to ensure internal and external communications can be supported or leaving the system as is and suggesting alternative implementation strategies.

SSM offers a better understanding of the problem and solutions available. The analysis looks for rational, evidence-based advice: The assessments look for in-depth understanding of the problem in a context supported by facts and data, and an analysis of the solutions available based on this insight, which will inform and support the decision-making and advocacy. The assessments allow for skepticism, expertise, and independence.

The purpose of this method is to inform and support alternative policy choices. The benefit of the method is that it can support the community's values, goals, and interests.

SSM is a systemic approach for addressing complex problematic situations that was developed by Peter Checkland and his colleagues at Lancaster University in the

136 Peter Checkland, *Systems Thinking, Systems Practice*. New Jersey: John Wiley & Sons, 1999.

1970s. It is designed to shape interventions in the problematic situations encountered in management, organizational and policy contexts, where there are often no straightforward problems or easy solutions. Though informed by systems engineering approaches, it breaks with them by recognizing the central importance of perspective or world-view in social situations. It differs significantly from the "systems science" approaches developed in the 1960s, and is more reflective of action research in its philosophy and approach.

6. Criteria Used to Judge Alternatives

The measure of effectiveness is difficult, since the options are modeled with little opportunities for field testing, thus effectively preventing the collection of a great deal of quantitative data on the benefits of any of the options. Therefore, the criteria for judging the success of each of the models must include an estimate of effectiveness of promoting the primary goal of the incident command system, that being to serve the needs of the community and to protect lives and save property. In addition, measures of effectiveness are judged based on how the options positively or negatively impact the assessment factors

Models that seek changes in the current incident command system are measured as to how they affect command, control, communication, coordination, and cooperation within the system. A matrix of the tenants of the ICS is used, and the models are evaluated in each category.

ICS is based on the following 14 proven management characteristics[137] that contribute to the strength and efficiency of the overall system:

Common Terminology: ICS establishes common terminology that allows diverse incident management and support organizations to work together across a wide variety of incident management functions and hazard scenarios. The models are assessed as to their ability to improve the use of common terminology throughout the incident and the ability to utilize that terminology throughout the incident theater of operations.

---

[137] Department of Homeland Security, "National Incident Management System," 2008. Available at http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf. 25.

Modular Organization: The ICS organizational structure develops in a modular fashion based on the size and complexity of the incident, as well as the specifics of the hazard environment created by the incident. When needed, separate functional elements can be established, each of which may be further subdivided to enhance internal organizational management and external coordination. Responsibility for the establishment and expansion of the ICS modular organization ultimately rests with Incident Command, which bases the ICS organization on the requirements of the situation. As incident complexity increases, the organization expands from the top down as functional responsibilities are delegated. Concurrently with structural expansion, the number of management and supervisory positions expands to address the requirements of the incident adequately. The assessment evaluates whether the models enhance or detract from the structure's ability to develop in a modular fashion.

Management by Objectives: Management by objectives is communicated throughout the entire ICS organization and includes:

- Establishing overarching incident objectives.
- Developing strategies based on overarching incident objectives.
- Developing and issuing assignments, plans, procedures, and protocols.
- Establishing specific, measurable tactics or tasks for various incident management functional activities, and directing efforts to accomplish them, in support of defined strategies.
- Documenting results to measure performance and facilitate corrective actions.

Peter Drucker is credited with being the first person to publish the concept of (and coin the term) "management by objectives" (MBO). The key to Drucker's concept of MBO is that subordinates play a major role in setting their own objectives rather than simply receiving objectives from superiors. The assessment determines whether the

modeled options enhance the ability to create overarching incident objectives, the strategies and the specific, measurable tactics, or tasks for various incident management functional activities.[138]

Incident Action Planning: Centralized, coordinated incident action planning should guide all response activities. An Incident Action Plan (IAP) provides a concise, coherent means of capturing and communicating the overall incident priorities, objectives, and strategies in the contexts of both operational and support activities. Every incident must have an action plan. However, not all incidents require written plans. The need for written plans and attachments is based on the requirements of the incident and the decision of the Incident Commander or Unified Command. Most initial response operations are not captured with a formal IAP. However, if an incident is likely to extend beyond one operational period, become more complex, or involve multiple jurisdictions and/or agencies, preparing a written IAP will become increasingly important to maintain effective, efficient, and safe operations.

Action planning demands a multi-step, concentrated, ongoing process based on management commitment, time, and accountability. No single strategy or process will be right for every incident. A structured approach built with an understanding of the specific needs of the organization is essential for success. Effective planning usually works from well-defined and explicitly stated objectives. It requires analysis of organizational strengths and weaknesses and environmental opportunities and threats, it produces alternative solutions, it chooses a solution, and it states how the solution will be implemented. The assessment determines whether the models enhance or detract from the ability to develop and implement incident action plans, in addition to contingency and emergency plans.

Manageable Span of Control: Span of control refers to the way relations are structured between leaders and subordinates in the organization. A wide span of control

---

138 Ronald G. Greenwood, "Management by Objectives: As Developed by Peter Drucker, Assisted by Harold Smiddy," *Academy of Management. The Academy of Management Review (pre-1986);* April 1981; 6.

exists when a manager oversees many subordinates; a narrow span of control exists when a manager oversees few subordinates. Span of control is the key to effective and efficient incident management.[139] Supervisors must be able to adequately supervise and control their subordinates, as well as communicate with and manage all resources under their supervision. Meyer states that the three variables that demand attention when setting span of control are diversity of tasks, organizational size and space, and instability. These variables create heterogeneous demands on an organization and prevent the use of wide spans of control.[140]

In ICS, the span of control of any individual with incident management supervisory responsibility should range from 3 to 7 subordinates, with 5 being optimal. In tactical operations, three people are a practical span of control. Span of control also applies to the supervision of locations and units as well as individuals. Consider an incident that begins in a single locale and expands into several states. During a large-scale law enforcement operation, 8 to 10 subordinates may be optimal. The type of incident, nature of the task, hazards and safety factors, and distances between personnel and resources all influence span-of-control considerations. At the national level, the span of control begins to expand to criticality

This assessment determines whether the models expand the span of control of any significant position within the ICS. Widening of the span of control would be considered as a negative finding, whereas, reduction of the span of control is considered a positive finding.

Incident Facilities and Locations: Various types of operational support facilities are established in the vicinity of an incident, depending on its size and complexity, to accomplish a variety of purposes. The Incident Command will direct the identification and location of facilities based on the requirements of the situation. Typical designated facilities include Incident Command Posts, Bases, Camps, Staging Areas, mass casualty

139 Department of Homeland Security. "*National Incident Management System*, 2008. 47.

140 Kenneth Meier and John M; Bohte, "Span of Control and Public Organizations: Implementing Luther Gulick's Research Design." *Public Administration Review* 63, no. 1 (February 2003): 61.

triage areas, point-of-distribution sites, and others as required. The assessment determines whether the model will require the establishment of additional facilities or support to additional locations. The requirement to establish additional facilities to support the models would be a negative finding.

Comprehensive Resource Management: Maintaining an accurate and up-to-date picture of resource utilization is a critical component of incident management and emergency response. Resources identified in this way include personnel, teams, equipment, supplies, and facilities available or potentially available for assignment or allocation. This assessment determines whether the policy options facilitate resource management.

Integrated Communications: Incident communications are facilitated through the development and use of a common communications plan and interoperable communications processes and architectures. This integrated approach links the operational and support units of the various agencies involved. It is necessary to maintain communications connectivity and discipline and to enable common situational awareness and interaction. The models assess the ability of the ICS to facilitate integrated communications.

Establishment and Transfer of Command: The command function must be clearly established from the beginning of any incident operations. The agency with primary jurisdictional authority over the incident designates the individual at the scene responsible for establishing command. When command is transferred, the process must include a briefing that captures all essential information for continuing safe and effective operations. The evaluation determines whether a model enhances or detracts from the ability to establish or transfer command.

Chain of Command and Unity of Command: Chain of command refers to the orderly line of authority within the ranks of the incident management organization.

Unity of command means that all individuals have a designated supervisor to whom they report at the scene of the incident. These principles clarify reporting

relationships and eliminate the confusion caused by multiple, conflicting directives. Incident managers at all levels must be able to direct the actions of all personnel under their supervision. The models assess the ability of the ICS to support or enhance the chain of command.

Unified Command: In incidents involving multiple jurisdictions, a single jurisdiction with multiagency involvement, or multiple jurisdictions with multiagency involvement. Unified Command allows agencies with different legal, geographic, and functional authorities and responsibilities to work together effectively without affecting individual agency authority, responsibility, or accountability. The assessment determines whether the models facilitate or prevent the development of unified command.

Accountability: Effective accountability of resources at all jurisdictional levels and within individual functional areas during incident operations is essential. Adherence to the following ICS principles and processes helps to ensure accountability:

- Resource Check-In/Check-Out Procedures
- Incident Action Planning
- Unity of Command
- Personal Responsibility
- Span of Control
- Resource Tracking

Dispatch/Deployment: Resources should respond only when requested or when dispatched by an appropriate authority through established resource management systems. Resources not requested must refrain from spontaneous deployment to avoid overburdening the recipient and compounding accountability challenges. The evaluation determines whether the models alter the current abilities of the ICS to dispatch or deploy resources.

Information and Intelligence Management: The incident management organization must establish a process for gathering, analyzing, assessing, sharing, and

managing incident-related information and intelligence. Effective emergency management and incident response activities rely on flexible communications and information systems that provide a common operating picture to emergency management/response personnel.[141] The incident management organization must establish a process for gathering, analyzing, assessing, sharing, and managing incident-related information and intelligence.

During an incident, this integrated approach to information and intelligence management links the operational and support units of the various organizations to maintain communications connectivity and situational awareness. These systems are to be used to provide decision support information to managers by collecting, updating, and processing data, and tracking resources. They enhance resource status information flow and provide real-time data in a fast-paced environment where different jurisdictions, emergency management/response personnel, and their affiliated organizations are managing different aspects of the incident and should coordinate their efforts. Examples of management information systems include resource tracking, transportation tracking, inventory management, reporting, and geographical information systems. The selection and use of systems for resource management should be based on the identification of the information needs within a jurisdiction.

In addition, this assessment evaluates the ability to implement the additional information-sharing network necessary for incidents of the twenty-first century.

This assessment determines whether the policy options facilitate or detract from meeting each of these ICS tenants. The models are assessed on their ability to create preparedness, planning, equipment, systems, and protocols necessary to achieve integrated voice and data communications within the incident and externally. The policy options may hinder or ease the ability to create management structures to meet the needs of the incident and each will be weighted accordingly.

[141] Department of Homeland Security "National Incident Management System," 2008. 35.

The following criteria are assessed to evaluate the estimated expectation for success of each of the models discussed to address the problem:

Effectiveness: Effectiveness can be a difficult to defined term; however, in this context, effectiveness shall be defined as the ability of the ICS to implement an incident action plan. The ability to implement the incident action plan depends on having a management structure to meet all the incident objectives. The models are evaluated for their ability to assist in the implementation of the incident action plan.

Cost: The cost of any change to the NIMS and the ICS will be substantial to federal, state and local agencies. However, the relative differences between a large change and a minor change will not be significant. Responders will require updated training, and materials will have to be updated and re-published. Large relative costs will be a negative finding.

Externalities: Externalities *will be defined as possible constraints that* may hinder the adoption or implementation of policies *preventing adaption. Examples of* Externalities may include, but not be limited to, legality or institutional lethargy. The assessment looks at how acceptable is the option to different people (e.g., government, citizens). Is the option legal? To what extent does the option provide a good solution beyond the short term? How quickly and easily can the solution be put in place?

Political Acceptability: Political Acceptability is the political will to implement the policy options changes. The political acceptability of changes to NIMS will be a significant issue with larger changes to ICS requiring greater efforts to assure implementation. Political acceptability will be the national general attitude towards acceptance without consideration of the local, regional, or statewide variations.

Institutional Lethargy: Institutional Lethargy is the instructional resistance to change. The ICS was mandated for use by all public safety agencies with HSPD 5 in 2003. Since then, all public safety agencies have been required to participate in training and certifications. This has created a large base of ICS users that is just beginning to fully implement and understand the ICS. In addition, this large user base creates a large pool of

potentially disenfranchised users if changes are made within short intervals. Significant changes now could have a disrupting effect. In order to counter this effect, changes need to be well explained and justified. The shear inertia of the user base will serve to inhibit changes.

In addition, the following adaptability criteria is assessed

Adaptable to any emergency: A key component of the ICS is in its ability to be scalable to any size incident. The assessment determines whether the policy options enhance that scalability to any emergency or detract.

Adaptable to any agency: Another key component of ICS is that is can be utilized as an all-risk system for all incident types and agencies. The assessment determines whether the policy options assist or hinder various agencies and agency types to implement the changed ICS.

Adaptable over time: ICS has the ability to grow, change, and contract as the needs of the incident change. This assessment determines whether that ability has been enhanced by the models.

Integrated into NIMS: The assessments determine whether the models fit within the conventions and intentions of NIMS and ICS. The models will be assessed utilizing a purist NIMS and ICS mindset.

The following are examples of the metric that assess how the options address the system requirements for an effective operation. The full metrics can be found in the Appendix.

Table 1. Adaptability Criteria

System Requirement	Model 1	Model 2	Model 3
Adaptable to any emergency			
Adaptable to any Agency			
Expandable			
Adaptable over time			
Integrated into NIMS			

The following matrix accesses the estimated expectation for success of each of the policy options discussed to address the problem:

Table 2. Criteria Measuring Success

System Requirement	Model 1	Model 2	Model 3
Effectiveness			
Cost			
Externalities			
Political Acceptability			

Another metric assesses how the options address the goals and key components of the ICS.

Table 3. Key Components

System Requirement	Model 1	Model 2	Model 3
14 goals and key components described above			

7. Comparison of Models

By utilizing the above metrics, we will be able to determine the best option and develop recommendations. These recommendations will also have considered the most likely recommendations of success.

Metrics are assessed utilizing a scale of 1 to 9, with 9 offering the most improvement over the current system. A rating of 5 will define a neutral benefit (no change) and 1 will be signifying a reduction from the current practice.

Chapter V explores three alternative solutions and their application towards improving communications. Following chapters discuss the three alternative models and begin the systematic comparisons.

V. DESCRIPTION OF ALTERNATIVE SOLUTIONS

A. INTRODUCTION

This chapter describes the alternative solutions identified for modeling. Alternative solutions for addressing the ICS communications problem would involve restructuring the system to make communications a priority and react to newer technologies. Restructuring may take alternative forms and each contains drawbacks. The option of maintaining the status quo also exists as a counter-point to more aggressive actions. This chapter does not delve into the advantages or disadvantages in each option. The analysis is discussed in later chapters.

Three models were chosen identify tentative solutions to the internal and external communication issues. The Communications Unit develops and maintains internal communications and any solution must include that unit. Similarly, external communications are handled by the PIO, and any solution must facilitate the PIO's functions. The third model combines the functions into one section working for the IC. The models are intended to work within NIMS and cause the least disruptions to the concepts and structures of the ICS. Other models could be developed; however, the three discussed provide the most effective enhancements while maintaining ICS integrity.

1. Model 1—Expanding Communications Unit Within the Logistics Section

This option would expand the Communications Unit within the Logistics, Service Branch to include all current and future internal communications functions. The Public Information Officer remains on the Incident Commander's command staff and the function of public information remains as is. The expanded Communication Unit's job functions would be defined to include all of the incident's current and future expectations.

The Logistics Section is responsible for all service requirements needed to facilitate effective and efficient incident management, including establishing

communications and information technology support. Incident communications are facilitated through the development and use of a common communications plan and interoperable communications processes and architectures. However, current trends and technologies are expanding communication beyond traditional voice radio systems. These trends include video, voice over IP, data, and Internet access systems.

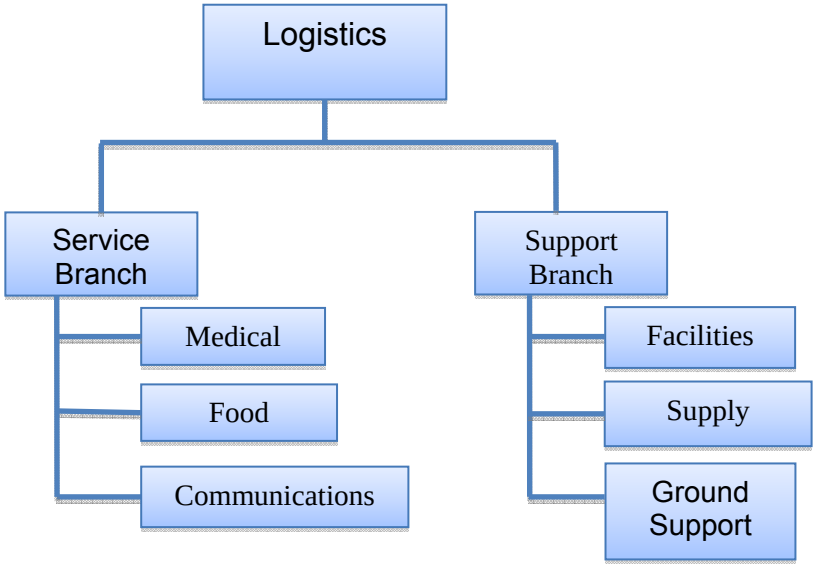

Figure 1. Logistics Section

The expanded Communication Unit will be responsible for all of the current duties but they will be expanded to include emerging technologies of video, data and Internet systems for the incident. Further definitions are discussed in Chapter VI.

The Communication Unit will develop a common communications plan. Preparedness planning will be the responsibility of the Communications Unit to address the equipment, systems, and protocols necessary to achieve integrated voice and data communications.[142] The integrated approach of the Communication Unit will link the

[142] Department of Homeland Security "National Incident Management System 2008," 48.

operational and support units of the various agencies involved and are necessary to maintain communications connectivity and discipline and to enable common situational awareness and interaction.

The expanded Communications Unit will be responsible for developing and maintaining new technologies, including Internet and email, data, instant messaging, and global information systems (GIS). The benefits of these systems would outweigh the expected costs. The expanded Communications Unit will develop, support, and maintain three main strategic functions: voice radio, data, and video. Within these systems are new tactical technologies that will facilitate new communications. These technologies include but are not limited to: instant text messaging, email, Internet capable of web-enabled applications and social media, and global information systems.

Highlights of the expected benefits from these new technologies for the incident include the ability for a commander to send messages instantaneously to all responders in the field by utilizing a telephone or data network would be invaluable. Changes in weather, changes in incident situations, or changes in orders could be relayed instantly to all members. The incident commander would be able to email communications and documents to any or all the responders or other stake holders. These documents include incident action plans, significant maps, and situation reports. In addition, email systems are capable of forwarding messages to other needed parties and maintaining copies of email for later actions and incident histories. By utilizing social media, the incident can utilize another method to send messages instantaneously to all responders in the field. The ability to instantaneously communicate with field resources will improve operational effectiveness and improve responder safety.

For the Planning Section the benefits of Internet, social networking, and instant communications would be high. The Planning Section is responsible for developing situational awareness and applying it towards operational plans. The principal methods are a bottom-up concept collecting data, developing information, gaining understanding, and applying understanding to current objectives. The data collection function provides the data required to gain situational awareness. In the ICS, planning is the function that

transforms the overall understanding produced by the situational awareness into orders. Instant messaging has the ability to collect data directly from field resources and can greatly facilitate planning.

Social media systems have become an important method of collecting situational awareness information from resources apart from responders. This was displayed in both the Japanese Tsunami and the Mumbai attacks. Accounts of these events have made the monitoring of social media sites almost mandatory.[143] [144] The information that can be gathered from social media will include videos and pictures from all around the incident, status of infrastructure, and links to other relevant data.

It does not seem unreasonable to assume that products relating to the situational awareness would improve the quality of incident command. It would presumably lead to a more disciplined, yet more creative, awareness process and provide a clearer input to the planning function. As noted above, today's products, combined with the commander's intent, may allow the creation of alternative solutions.

In essence, emerging technologies will greatly enhance the steps required for controlling an incident, monitoring the situation, developing situational awareness, developing courses of action, decision making that selects among the courses of action, developing and promulgating guidance to implement those decisions, and establishing mechanisms for feedback that allow the cycle to be continuous by monitoring the situation during implementation. New technologies are going to be essential in meeting these steps and the expanded Communication Unit will be required to implement the technologies.

The expanded Communications Unit will be scalable, in accordance with ICS principles. On incidents with a single agency, with the agency's single dispatch and

---

[143] Harry Wallop, "Japan Earthquake: How Twitter and Facebook Helped" *The Telegraph*, March 13, 2011. Available at http://www.telegraph.co.uk/technology/twitter/8379101/Japan-earthquake-how-Twitter-and-Facebook-helped.html.

[144] Stephanie Busari, "Tweeting the Terror: How Social Media Reacted to Mumbai" *CNN World* November 27, 2008. Available at http://articles.cnn.com/2008-11-27/world/mumbai.twitter_1_twitter-tweet-terror-attacks?_s=PM:WORLD.

tactical radio frequency, the Communications Unit may be a low priority. As the incident grows and other agencies and frequencies are required, the Communication Unit may be established. This unit may only deal with voice radio. Additional radio operators may be assigned. As the incident continues to grow and additional technicians are added, video and data centers may be established to maintain the span of control. These centers will be staffed with managers and technicians. An example of a full staffed Communications Unit can be seen in Figure 2.

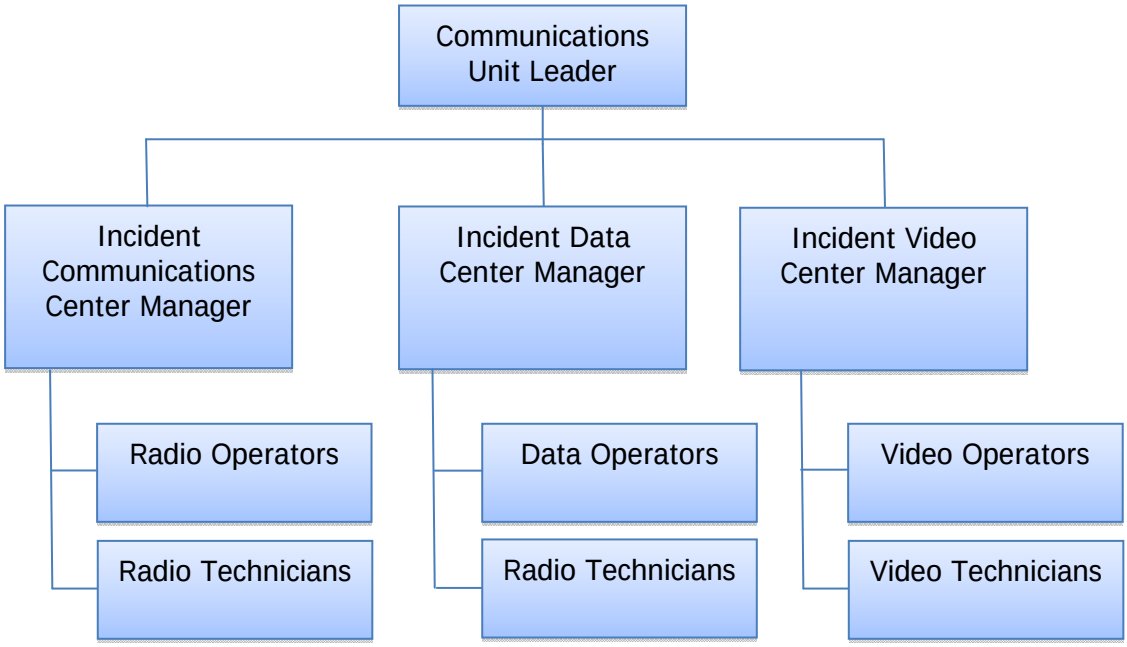

Figure 2. Expanded Communications Unit

2. Model 2—Expanding the Public Information Officer Role

In the second model, external communication will continue to be handled by the Public Information Officer. The Public Information Officer would continue to support the incident command structure as a member of the Command staff and advise the Incident Commander/Unified Commander on all public information matters relating to the management of the incident. The position would be given specific responsibilities and

tasks that the defined Public Information Officer would be required to complete. This option would keep the internal communication support functions within the Communications Unit within Logistics.

The Public Information Officer would continue to be responsible for communicating with the public, media, and/or coordinating with other agencies, as necessary, with incident-related information or requirements. The Public Information Officer would be responsible for developing and releasing information about the incident to the news media, incident personnel, and other appropriate agencies and organizations. Depending on the size or complexity of the incident, a lead Public Information Officer would be assigned for each incident and may have assistants, as necessary, including supporting Public Information Officers representing other responding agencies or jurisdictions. As a member of the Command staff, the Public Information Officer may be assigned numerous Assistant Public Information Officers to fill the various responsibilities as necessary.

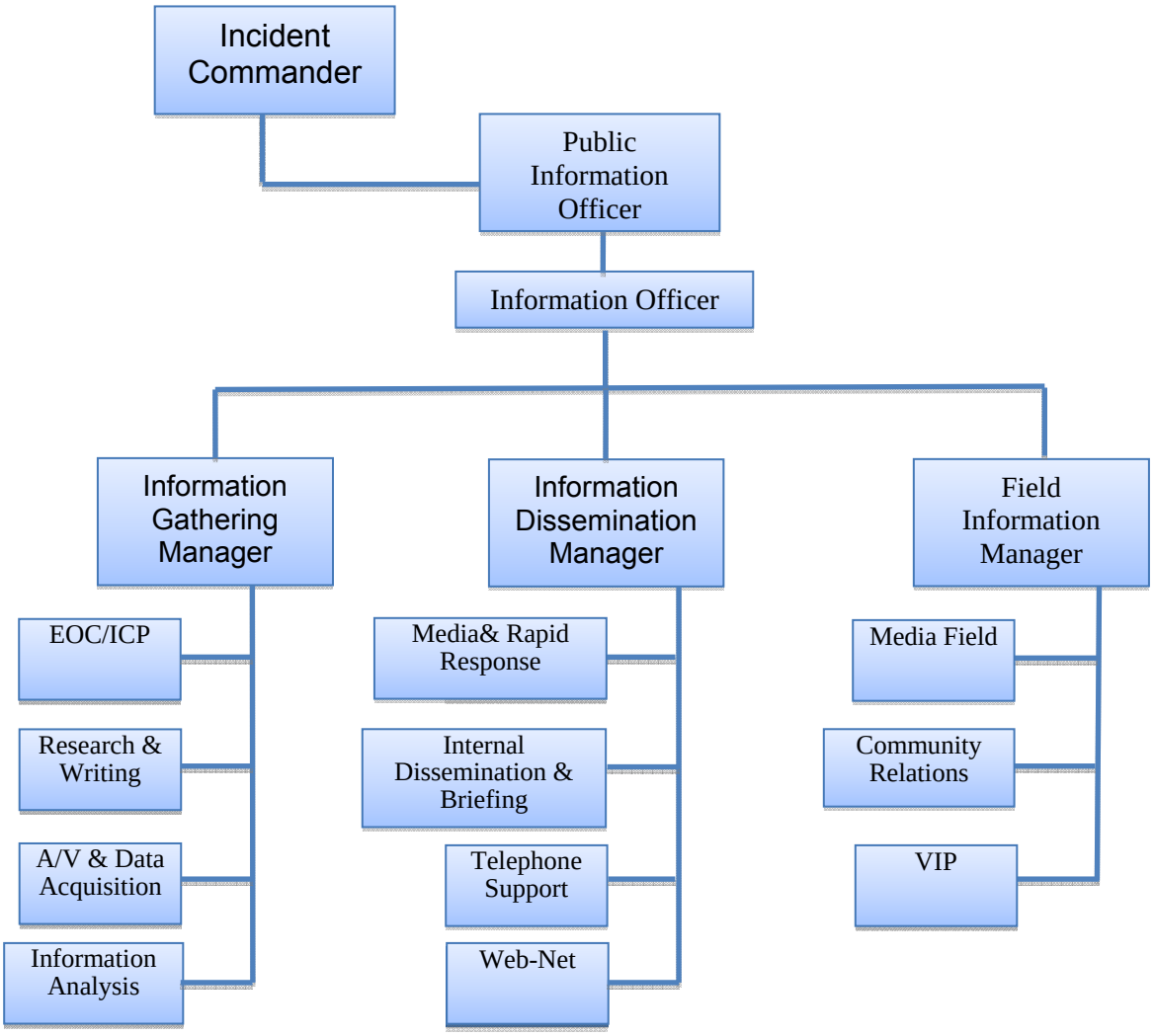

Figure 3. Expanded Public Information Officer Role

The Public Information Officer will supervise one assistant, designated as the Information Officer. The Information Officer manages the information flow in and out of the command post. The Information Officer will gather, confirm, clarify, and forward the information to the Public Information Officer for approval and dissemination and then on to internal distribution channels. In addition, the Information Officer will coordinate with Logistics to ensure that the communication infrastructure is in place and can support information collection and distribution. In expanded incidents, additional assistants will

be assigned to handle information gathering, information dissemination, and field information functions. Additional explanations of duties and responsibilities of the expanded Public Information Officer will be included in Chapter VI.

Information communications strategies and planning are essential to all aspects of public information. The Public Information Officer will be responsible for plans that would include processes, protocols, and procedures involving the development of draft news releases, media lists, and contact information for elected/appointed officials, community leaders, private-sector organizations, and public service organizations to facilitate the dissemination of accurate, consistent, accessible, and timely public information.

Similar to the expanded Communications Unit, the expanded PIO will be scalable, in accordance with ICS principles. On incidents with a single agency, a single PIO may be required. As the incident grows and other agencies and frequencies are required, assistants may be assigned as needed. As the incident continues to grow in size or complexity, the expanded PIO may be utilized. The expanded PIO will have managers to assist with the major functions of information gathering and information dissemination. In addition, a key component added is a manager to keep field resources informed.

The Information Gathering Manager will be responsible for the collection and analysis of the information. Collections should include incident command post/chain of command sources, news video and reports, email and other newer technologies. These technologies include social media and other Internet sites. As stated above, these sources are developing into critical information sources that cannot be ignored. One of the main reasons to foster social networks is the operational power of having shared awareness, a shared understanding of the current situation, a shared sense of the operational implications, and a shared intent about the direction of the incident. The ability of the Information Gathering Manager to collect and analyze the feeds from various sources will ensure that the information is vetted and disseminated rapidly. This creates a symbiotic relationship that will continue to grow.

Additional members can be assigned to the Information Gathering Manager as needed. A key component of the expanded PIO is coordination with the local, county or state Emergency Operations Center (EOC). In conjunction with the EOC, Joint Information Centers may be established. Additional members may be assigned to the expanded PIO to facilitate interaction with the EOC. These members will fulfill the functions of EOC/Incident Command Post (ICP) coordination and data collection. Other members may be assigned to writing and research, audio/video and data acquisition, and information analysis.

The information distribution functions will be the responsibility of the Information Dissemination Manager. The Information Dissemination Manager will work with the various information distribution channels including television, radio and print media, as well as emerging technologies of social media and other Internet outlets. The Information Dissemination Manager will be responsible for setting up the media briefings and coordinating any rapid media activities. Telephone support and Internet support personnel can also be assigned to facilitate information flows.

A critical component missing from the current ICS is field information, getting accurate incident information to other field resources. This function will be handled in the expanded PIO by the Field Information Manager. The Field Information Manger will disseminate the prepared information and deliver it to the responders and other internal stakeholders. Through the application of new technologies, this can be accomplished through email or instant messaging. The prospect of having field members with situational awareness of the incident is an important part of gaining perspective and ownership of their part in it.

Another component is VIP support. At every large incident, elected officials have concerns that only personal visits can address. This has the tendency to detract from the incident commander’s attention and time. The Field Information Manger will be responsible for supporting VIPs at the incident, ensuring that they receive update incident information and coordinate media briefings with the PIO.

3. Model 3—Creating a Communications Section

The ICS has four sections: Operations, Planning, Logistics, and Finance. Deep within the Logistics section, under the Support Branch, resides the Communications Unit. External Communication is handled by a member of the Command Staff, the Public Information Officer. While the Public Information Officer may have assistants assigned on an as-needed basis, a clear, defined organization is not defined.

It may be instructional to discuss the differences between a section and unit. A section in the ICS is a large organizational component that contains various divisions, groups, and units. It the span of control warrants, the section may be broken into branches. A unit is a smaller group of single resources. The following figure displays the general positions within the ICS hierarchy:

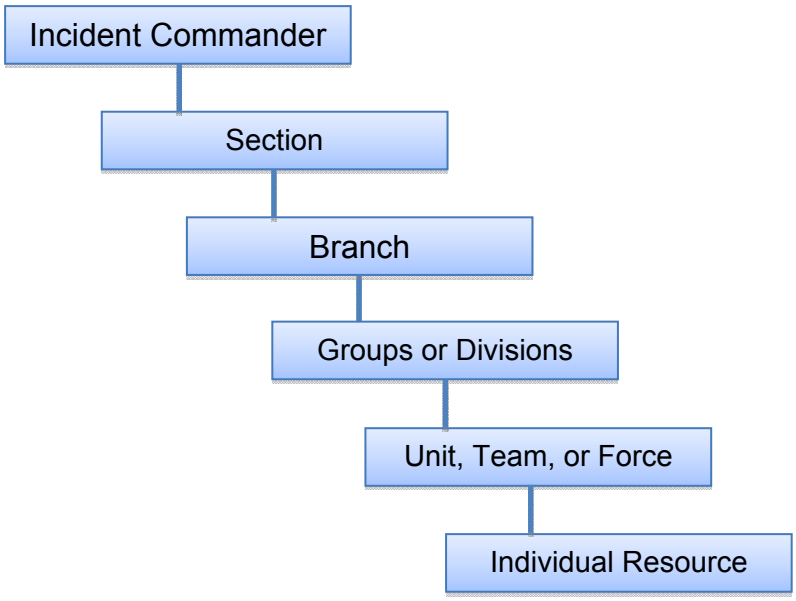

Figure 4. ICS Hierarchy

The commander of a section is called Chief and the commander of a Branch is called Director. A Division is commanded by a Supervisor and can be arranged by geography, along jurisdictional lines if necessary. A Group, commanded by a Supervisor,

is arranged for a purpose, along agency lines if necessary, or based on the makeup of the resources within the Group. A Unit, Team, or Force is commanded by a Leader, for example the Communications Unit is commanded by the Communications Unit Leader. A Strike Team is composed of same resources (four ambulances, for instance) while a Task Force is composed of different types of resources (one ambulance, two fire trucks, and a police car, for instance). Individual Resources are the smallest level within ICS and usually refers to a single person or piece of equipment. It can refer to a piece of equipment *and* operator, and less often to multiple people working together.

This model is to merge all communications functions into one section directly under the Incident Commander. Within the Communications Section, all information collection, creation, and delivery systems will be combined into one section reporting directly to the IC. The importance of creating a Section is to move communication up to one of the five key components that the IC must coordinate. This raises communications to the level equal of operations, Planning, Logistics, and Finance.

This section would handle all internal and external communications functions, with each having a separate branch. This option argues that the communication as a whole should be given increased prominence through the creation of a separate function, sitting alongside, rather than underneath, Planning, Operations and Logistics, and reporting directly to the Incident Commander.

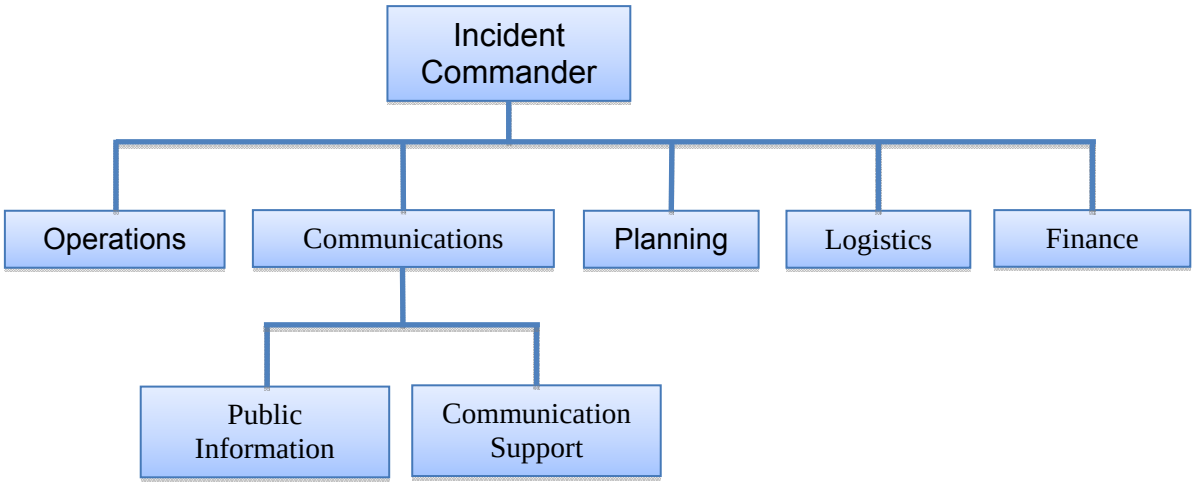

Figure 5. Communications Section

In this option, all communication would be the responsibility of the Communication Section Chief. This Section Chief would be responsible for establishing communication networks for voice, video, and data within the incident. In addition, the Communication Section Chief would be responsible for developing the content and providing external communications to the media, elected official, and the public. Inter-incident communication networks will be established and maintained by the Communication Support Branch. Under this branch, various groups, divisions and units may be established to facilitate radio, video, data, and Internet systems. These systems will carry the information content developed by the incident to the necessary end users.

The Public Information Officer, whose focus is community information and warnings, is a critical addition to the Communications Section. The Public Information Officer will maintain the responsibility for gathering, analyzing, and confirming incident information and the delivery to incident stakeholders. The Public Information Officer will create coordinated and consistent messages by collaborating to identify key information that needs to be communicated to the public. As such, the Public Information Officer will

not be separated from the information collection and distribution functions. Formulation of warnings that are accurate and timely and take full account of the situation on the incident depends on an adequate flow of information; this flow of information is the responsibility of the Public Information Branch. Multiple groups, divisions, and units can be established to support the Public Information Officer.

The Public Information Branch will be responsible for developing and deploying Joint Information Systems (JIS) and participating in Joint Information Centers (JIC). The JIC is a central location that facilitates operation of the JIS, where personnel with public information responsibilities perform critical emergency information functions, crisis communications, and public affairs functions. These systems will provide the mechanism to organize, integrate, and coordinate information to ensure timely, accurate, accessible, and consistent messaging across multiple jurisdictions and/or disciplines with Non-Government Organizations (NGO) and the private sector. The JIS will include the plans, protocols, procedures, and structures used to provide all public information in a complex incident. For smaller, less complex incidents Public Information Branch might consist of only one member, who will combine the roles of branch leader and Public Information Officer.

The described three options are not mutually exclusive. One, more, or a combination may be selected to fit the needs of future homeland security events. Expansion of the Communications Unit and expansion of the PIO may work concurrently.

In the following chapter, the three models are assessed individually to evaluate their project effectiveness in reducing the communication issues, while adhering to the concepts of the ICS.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. PROJECTED OUTCOMES FROM ALTERNATIVE SOLUTIONS

A. INTRODUCTION

Herein, the research begins the structured debate about the desirable and feasible change. Utilizing the matrix developed of the key concepts, adaptability criteria, and criteria measuring success assessed against the models, the research identifies the optimum models to recommend. The recommendations will also have considered the most likely recommendations of success.

The research utilizes a single-impact analysis on each of the 14 key components, 5 adaptability criteria and 4 criteria measuring success. Single-impact analysis is a method of codifying simple cause and effect links in the format of a matrix. Single-impact analysis uses assessments in a one directional study of a complex system. When conducting the single impact analysis, it was first necessary to identify and develop the alternative models for assessment and the measurable components of each model. For this evaluation, the 14 key components of the ICS were selected to ensure that the models retained the original concepts of the ICS. In addition, the 5 adaptability criteria and 4 criteria measuring success were identified as components estimating expectation for success of each of the policy options. The components are then assessed individually for each model as to how well they will work in each scenario.[145] This method was selected to isolate the variables for review, and measure the effects based on the definitions of the component in Chapter IV. Each effect is given a number based on the level of impact. Metrics are assessed utilizing a scale of 1 to 9, with 9 offering the most improvement over the current system. A rating of 5 will define a neutral benefit (no change) and 1 will be signifying a reduction from the current practice. The assessments are found in Tables 4, 5, and the Appendix.

[145] Mats Lindgren and Hans Bandhold, *Scenario Planning: The Link Between Future and Strategy*. New York: Palgrave Macmillan, 2003. 149.

The findings displayed in Table 4 show that when assessing the three models against the 14 key components identified in the development of ICS, Model 3, Creating a Communications Section showed the most improvement over the current system. In addition, Model 1, Expanding the Communications Unit and Model 2, Expanded PIO Role, displayed improvement over the current.

The assessments of the 5 adaptability criteria and 4 criteria measuring success are displayed in Table 5. These criteria, in many ways, may be more significant than the 14 key components. Costs, externalities, and political will may have greater impacts into the adaption of the recommendations than other factors. Each finding is discussed in detail below for the three models.

1. Model 1—Expanding Communications Unit Within the Logistics Section

All units on an incident require effective and efficient information, and that information traverses through communication networks established by the Communications Unit. Since all units on an incident contribute to the establishment of situational awareness of the operational environment, it is important that they be able to transmit this situational awareness and the history of their own activities to their commanding officers. Conversely, it is imperative that operating units receive relevant and up-to-date information on the current situation, the required mission information and the intended effect. In addition, the incident commander must receive feedback to the plans being implemented in order to create plans for the next operational periods. In order to accomplish this, the Communications Unit establishes networks.

By expanding the Communications Unit within the Logistics Section, we can expect to create a more robust internal communication support function. The Communications Unit will develop and support the various communication channels of the incident. In addition, the Communications Unit will develop and support the external communication channels to facilitate external communications. These channels and

networks will include, but not be limited to, voice, video, and data. Also, Internet functionality must be developed and maintained to capitalize on off-site data sources and social networks.

The assessment of the 14 key components, 5 adaptability criteria and 4 criteria measuring success is based on the definitions outlined in Chapter IV. The current ICS structure has been identified as having a baseline of 5. Improvements from the current structure will be denoted with higher numbers, and conversely, lower numbers display a reduction.

Common Terminology–5 The expanded Communications Unit will have a minimal impact on the use or application of common terminology and plain language. The use of plain language (clear text) in emergency management and incident response is a matter of public safety, especially the safety of emergency management/response personnel and those affected by the incident. Common terminology and plain language are parts of the content of the systems and should not be affected.

Modular Organization–6 The expanded Communications Unit will facilitate a modular organization. The ICS organizational structure develops in a modular fashion based on the size and complexity of the incident and this unit can be expanded as the incident is needed. On smaller, single agency incidents where only voice radio is needed, those components can be built out. In larger incidents, all positions may be filled.

Management by Objectives–7 The expanded Communications Unit will improve on the ability to create and implement management by objectives. Key objectives always involve developing and maintaining communication networks to ensure responder and public safety. The expansion of the Communication Unit will facilitate accomplishing those objectives.

Incident Action Planning–6 The expanded Communications Unit will improve the ability to develop and implement incident action plans, in addition to contingency and emergency plans, however, voice and data networks become increasing fragile as they grow increasing complex.

Manageable Span of Control–6 The Communications Unit is commanded by a Unit Leader. Reporting to the unit leader can be various positions, including but not limited to, radio technicians, video technicians, data technicians, and radio operators. Communications Unit staffing needs may vary according to the scope and scale of the incident. More radio operators, video, data, and radio technicians are needed as more agencies and responders are involved. Multiple communications units may be necessary due to geographical considerations.

The Incident Communications Center Manager, Data Center Manager, or Video Center Manager positions may be filled when the unit leader's span of control would be exceeded, either by the complexity of the incident, requiring an unusual degree of involvement in incident action planning, or by the number of technicians and radio operators assigned to the unit.

Incident Facilities and Locations–5 The expanded Communications Unit will have little effect on incident facilities and locations, other than the possibility of creating dispatch and data centers.

Comprehensive Resource Management–6 The expanded Communications Unit will facilitate resource status by allowing multiple methods to feed status to the Planning Section. Units would be able to utilize text messaging and email to update status.

Integrated Communications–8 The expanded Communications Unit will improve the ability of an incident to develop a common communications plan and interoperable communications processes and architectures. In addition, the utilization of video and data systems will also facilitate more integrated communications.

The Communications Unit is required to develop policies, procedures, and systems to keep the leaders informed of the size and scope of the emergency, and ensure that those systems are capable to convey information and orders to operating forces. The expanded Communications Unit will be responsible for all of those current duties, but will be enlarged to include emerging technologies of video, data, and Internet systems.

Establishment and Transfer of Command–5–The expanded Communications Unit will not alter the establishment and transfer of command. However, by establishing the hierarchical structure within the expanded communication unit, when addition Communication Technicians (COMT) or Radio Operators (RADO) are added, the Communications Unit Leader (COML) has the ability to add managers to maintain the span of control. This will facilitate and maintain the transfer of command.

Chain of Command and Unity of Command–5 The expanded Communications Unit will not alter the chain of command and unity of command. Communication technicians will continue to report to the communication unit leader or managers when established.

Unified Command–5 The expanded Communications Unit will not affect the ability of the incident to form under a unified command.

Accountability–5 The expanded Communications Unit will not affect accountability. In future applications, the use of new technologies to monitor responders will require addition networks. The expanded communication unit will be in the position the implement these newer technologies as they become available.

Dispatch/Deployment–5 The expanded Communications Unit will not change the ability of the unit to facilitate dispatch or deployment. These functions are currently facilitated by the communications unit and adding the networking functionality will not alter these functions.

Information and Intelligence Management–8 The expanded Communications Unit will improve on the incident's ability to move, store, and utilize information. Information and intelligence are the keystones of effective sense making, and the utilization of data and video networks, in addition to voice networks, will improve the channels for information flows.

The expanded Communications Unit will be responsible for developing and maintaining new technologies, including Internet and email, data, instant messaging and

global information systems. The benefits of these systems would outweigh the expected costs. Highlights of the expected benefits from these new technologies for the incident commander include:

The ability for a commander to utilize instant messaging to send messages instantaneously to all responders in the field utilizing a telephone or data network would be invaluable. Changes in weather, changes in incident situations, or changes in orders could be relayed instantly all members.

The incident commander would be able to email communications and documents to any or all the responders or other stake holders. These documents include incident action plans, significant maps, and situation reports. In addition, email systems are capable of forwarding messages to other needed parties, and maintaining copies of email for later actions and incident histories.

Utilizing social media, the incident commander can utilize another method to send messages instantaneously to all responders in the field. The ability to instantaneously communicate with field resources will improve operational effectiveness and improve responder safety.

For the Planning section, the benefits of Internet, social networking, and instant communications would be high. The Planning Section is responsible for developing situational awareness and applying it towards operational plans. The principal methods are a bottom-up concept collecting data, developing information, gaining understanding, and then applying understanding to current objectives.

Today's planning staff procedures provide examples of fulfilling the situational awareness function, and a first step in the research and development of better systems. More important, however, may be to think about the new ways of doing situational awareness that become possible with the new forms of technology.

The data collection function facilitated by instant messaging provides the data required to gain situational awareness. In the ICS, planning is the function that transforms the overall understanding produced by the situational awareness into orders.. However,

giving control to the data collection function is the most obvious way of creating information overload, while, on the other, pushing information to the planning section seems to be the best way of escaping the risk that important events are not detected. Striking the right balance here is the problem. It not obvious that there is a simple solution to this problem, and the best approach may well be a hybrid solution where the user exercises a high degree of control over what he or she receives, yet allows for urgent messages from the data collection function to be passed on.

Email systems will work parallel to the instant messaging systems in delivering and receiving messages. Messages and photographs taken in the field can be forwarded (logged and archived) to the planning section for instant updates of a field resources progress. These updates will be folded into the next operational plan without having to wait for units to come in off the line for debriefing.

Social media systems have become an important method of collecting situational awareness information from resources apart from responders. This was displayed in both the Japanese Tsunami and the Mumbai attacks. Accounts of these events have made the monitoring of social media sites almost mandatory.[146] [147] The information that can be gathered from social media will include videos and pictures from all around the incident, status of infrastructure, and links to other relevant data.

The development of applications for smart phones can further assist the planning section. Readers can be accessed so that any member with a smart phone can have a copy of the incident action plan or a field operations guide. The GPS functionality can support mapping duties, and photography will support data collection.

The development and proliferation of web-enabled applications will provide the incident with multitudes of capabilities. The ability of field resources to complete the

---

[146] Harry Wallop, "Japan Earthquake: How Twitter and Facebook Helped" *The Telegraph*, March 13, 2011. http://www.telegraph.co.uk/technology/twitter/8379101/Japan-earthquake-how-Twitter-and-Facebook-helped.html.

[147] Stephanie Busari, "Tweeting the Terror: How Social Media Reacted to Mumbai" *CNN World* November 27, 2008. http://articles.cnn.com/2008-11-27/world/mumbai.twitter_1_twitter-tweet-terror-attacks?_s=PM:WORLD.

required forms utilizing web-based forms would streamline the data collection and history functions. Mapping, vehicle location systems and other sense-making systems are other examples.

Through all these tools, the added functionality of the expanded Communications Units would increase information and intelligence management.

Adaptable to any Emergency–5 The expanded Communications Unit will be adaptable to any emergency. In keeping with the modular functionality of the ICS, the unit has the ability to grow and shrink to fit the incident's needs. This is not a change from the current communications unit.

Adaptable to any Agency–4 Adaptability of any agency may be hindered by adding requirements to new communications unit positions. Not all agencies have the ability or need to certify data technicians or video operators and this may limit that agency's ability to fill the positions. However, if the incident expands to require the expanded Communications Unit, those positions could be filled by normal procedures.

Expandable–7 The expanded Communications Unit will be expandable. From single agency incidents requiring only a couple of voice radio channels, to large, multi-jurisdictional incidents, the communications unit can be expanded as necessary. Filling the positions of data, or video manager will assist in maintaining the span of control.

Adaptable over time–5 The expanded Communications Unit will have the ability to grow, change, and contract as the needs of the incident change. This will not change from the current situation.

Integrated into NIMS–5 The expanded Communications Unit will integrate into NIMS. This is not a change from the current communications unit.

Effectiveness–7 The expanded Communications Unit will increase the ability to communicate and, therefore, increase the effectiveness of the ICS. The addition of data and video networks will better support the command and control of the incident.

It does not seem unreasonable to assume that products relating to the situational awareness would improve the quality of incident command. It would presumably lead to a more disciplined, yet more creative, awareness process, and provide a clearer input to the planning function. As noted above, today's products, combined with the commander's intent, may allow the creation of alternative solutions.

Internet networks, instant messaging, and email will improve the operations of logistics. Ordering would be expedited and record keeping would be facilitated. Email for messaging will prove to be invaluable.

In essence, emerging technologies will greatly enhance the steps required for controlling a incident, monitoring the situation, developing situational awareness, developing courses of action, decision making that selects among the courses of action, developing and promulgating guidance to implement those decisions, and establishing mechanisms for feedback that allow the cycle to be continuous by monitoring the situation during implementation. New technologies are going to be essential in meeting these steps, and the expanded Communication Unit will be staged to implement the technologies.

Externalities–6 The research can find no legal issues preventing the expanded Communications Unit. Institutional lethargy will be encountered for any change. The research has not found any other possible constraints that may hinder the adoption or implementation of policies preventing adaption.

Cost–7 The costs to the system for enhancing the Communications Unit will be minimal. Existing training curriculum may require some modifications, only if the discussion carries into expanded operations. The structure of the ICS will not be modified. Position descriptions and communication-specific training will be required.

Political Acceptability–8 The expanded Communications Unit will be politically acceptable. The net effect of the change is to add duties and responsibilities, additional

positions and new position descriptions to the existing communications unit. These positions will be needed only in larger incidents; therefore, impact to most operations is negligible.

However, there may be obstacles in moving this model forward. Institutional lethargy is a major hurdle. Making changes to the ICS, less than ten years since its implementation, may prove difficult. The ICS was mandated for use by all public safety agencies with HSPD 5 in 2003. Since then, all public safety agencies have been required to participate in training and certifications. This has created a large base of ICS users that is just beginning to fully implement and understand the ICS. In addition, this large user base creates a large pool of potentially disenfranchised users if changes are made within short intervals. Significant changes now could have a disrupting effect. In order to counter this effect, changes need to be well explained and justified. The shear inertia of the user base will serve to inhibit changes.

Culture and especially ideology in the existing public safety organizations do not encourage strategic change. The perpetuation of existing strategy is continuous unless forced by outside factors. Public safety agencies at best only tend to promote shifts in position within the organization's overall strategic perspective. In order to anticipate this, large strategic changes should be avoided. The recommendations can be forwarded as a shift in position rather than a strategic change in the ICS. Moving the existing communications functions can be displayed as a minor change consolidating functions within one section. The alternative may be too difficult to overcome due to resistance to strategic change. Mandated change from the National Integration Center is a goal, but total adoption and embracement of the change is the ultimate goal.

2. Model–2—Expanding the Public Information Officer Role.

The public expects information about the size, scope and impact of the incident and communication needs to flow to the community in a timely way to assist in the process of early warning and management of risk. Incident commanders needed to

provide the media and the community with information that is accurate, relevant, adequate, consistent, useful, and timely. This duty in many cases is assigned to the Public Information Officer.

The Public Information Officer is responsible for interfacing with the public, media, and other stakeholders with incident-related information. The Public Information Officer gathers, verifies, coordinates, and disseminates accurate, accessible, and timely information on the incident's cause, size, and current situation; resources committed; and other matters of general interest for both internal and external audiences.[148] For our discussions, public information consists of the processes, procedures, and systems to communicate timely, accurate, and accessible information on the incident's cause, size, and current situation to the public, responders, and additional stakeholders, directly and indirectly affected.

Model 2 explores the scenario of expanding and defining the Public Information Officer's duties and responsibilities and creating position descriptions for additional members working under that position to fill those duties. The PIO is an essential position; currently, that position is on the incident commander's command staff. The model's position is that the PIO remain on the command staff. However, as a member of the command staff, the PIO is allowed assistants. The ability to add managers to help reduce the span of control is not allowed under current ICS conventions. Therefore, when the PIO model is filled out, numerous assistants will be assigned.

Common Terminology–5 The expanded PIO model will not change the ability towards use of common terminology throughout the incident or the ability to utilize that terminology throughout.

Modular Organization–5 The expanded PIO model will facilitate a modular organization. The ICS organizational structure develops in a modular fashion based on the size and complexity of the incident and PIO functions can be expanded as the incident

148 Department of Homeland Security, "National Incident Management System 2008." 52.

is needed. On smaller, single agency incidents, where a single PIO is needed, that role can be filled. In larger incidents, all functions and positions may be filled.

Management by Objectives–7 The expanded PIO model will improve on the ability to create and implement management by objectives. Key objectives always involve developing and maintaining public information networks to ensure responder and public safety. The expansion of the PIO roles will facilitate accomplishing those objectives.

Incident Action Planning–6 The expanded PIO model will facilitate incident action planning. The expanded PIO will be able to develop media plans, in addition to contingency and emergency plans.

Manageable Span of Control–3 As a member of the command staff, the PIO is allowed to have assistants as direct reports. However, this does not allow for the creation of a hierarchal structure with managers and units under them. Technically, all the members under the PIO have the same ICS rank as assistant. This in turn violates the concepts of span of control. Creating the expanded PIO under the current configuration violates the established tenants of the ICS.

Incident Facilities and Locations–5 The expanded PIO model will have little impact on facilities and locations.

Comprehensive Resource Management–5 The expanded PIO model will have no impact on resource management.

Integrated Communications–6 The expanded PIO model will have minor impacts on integrated communications. The expanded PIO will utilize new technologies to reach the public and stakeholders. The expanded PIO will facilitate information flows to the incident commander and from the IC to the field resources. The utilization for new technologies of instant messaging, the FIM has the capability of developing overall situational awareness.

Establishment and Transfer of Command–5 The expanded PIO model will not affect the establishment or transfer of command. However, with the establishment of the expanded PIO function, the internal transfer of command may be facilitated.

Chain of Command and Unity of Command–4 The expanded PIO model will be negatively affect the chain of command. By assigning numerous assistants to the PIO, without the ability to assign rank, could impact the chain of command.

Unified Command–5 The expanded PIO model will not impact the concept of unified command.

Accountability–5 The expanded PIO model will not impact accountability.

Dispatch/Deployment–5 The expanded PIO model will not impact dispatch or deployment .

Information and Intelligence Management – 8 The expanded PIO model will greatly enhance information and intelligence. The ability to reach out to media, social media and the Internet will create additional capabilities and resources to gain situational awareness. The ability to keep field members informed through new technologies will also help information flows.

The PIO accomplished this mission through a four-step process. Gathering information is the first step in the process of getting information to the public and additional stakeholders. Information is collected from various sources, including the ICS chain of command, media accounts, and witnesses. The next step in the process is to verify the accuracy of the information that has been collected, by consulting the knowledgeable and credible sources. The next step in the process is to coordinate with other Public Information Officers who are part of the Joint Information System **(**JIS). These Public Information Officers include both those represented in the Joint Information Center (JIC) and those working from other locations as part of the JIS. Coordinating information involves developing and establishing key messages. Unified messages are crafted addressing all informational needs and are prioritized according to the overall incident strategy. Prior to releasing incident information, approval must be obtained from

incident commanders and others having approval authority. Once approved, the final step is dissemination using multiple media and methods. The PIO's primary mission includes getting accurate, consistent information to the stakeholders at the right time so they can make informed decisions.

The expanded PIO will greatly improve external communication and information flows. Situational awareness will be forwarded to the Planning Section for incorporation into operational plans. In addition, the utilization of social media's two-way communications to facilitate information flows will quickly create additional communication channels to get the incident commander's message to the communities affected. The size, scope, impact, and warnings can be distributed instantaneously. The effectiveness of the ICS will be increased due to increased situational awareness of the responders, stakeholders and the communities impacted.

Adaptable to any Emergency–6 The expanded PIO function will adapt to any size incident. At single agency events, the single PIO will continue to serve. As the incident grows, positions in the expanded PIO function can be filled.

Adaptable to any Agency–4 The expanded PIO model will require additional training for public information officers and data technicians. Much of this training is occurring; however, not all agencies have the needs or the capabilities for the expanded PIO.

Expandable–7 As stated above, the expanded PIO model will be expandable. The Model system is more capable of expansion than is the current model. The duties, roles, and responsibilities of public information are large, complex, and expanding. Current expectations of the public are growing. Therefore, this model suggests that in order to accomplish the duties, the PIO must be expanded to include additional defined positions. These positions can be filled, as is the ICS process, as the complexity and needs of the incident grow. Additional assistants can be added to fill needs. The PIO reports to the incident commander, and maintains the direct link as part of the command staff.

The expanded PIO will have managers to assist with the major functions of information gathering and information dissemination. In addition, a key component added is a manager to keep field resources informed.

The Information Gathering Manager (IGM) will be responsible for the collection and analysis of the information. Collections should include incident command post/chain of command sources, news video and reports, email, and other newer technologies. These technologies include social media and other Internet sites. As stated above, these sources are developing into critical information sources that cannot be ignored. One of the main reasons to foster social networks is the operational power of having shared awareness, a shared understanding of the current situation, a shared sense of the operational implications, and a shared intent about the direction of the incident. The ability of the IGM to collect and analyze the feeds from various sources will ensure that the information is vetted and disseminated rapidly. This creates a symbiotic relationship that will continue to grow.

Additional members can be assigned to the IGM as needed. These members will fulfill the functions of EOC/ICP data collection, writing and research, audio/video and data acquisition, and information analysis.

The information distribution functions will be the responsibility of the Information Dissemination Manager (IDM). The IDM will work with the various information distribution channels including television, radio, and print media, as well as emerging technologies of social media and other Internet outlets. The IDM will be responsible for setting up the media briefings and coordinating any rapid media activities. Telephone support and Internet support personnel can also be assigned to facilitate information flows.

A critical component missing from the current ICS is field information, getting accurate incident information to other field resources. This function will be handled in the expanded PIO by the Field Information Manger (FIM). The FIM will disseminate the prepared information and deliver it to the responders and other internal stakeholders. Through the application of new technologies, this can be accomplished through email or

instant messaging. The prospect of having field members with situational awareness of the incident is an important part of gaining perspective and ownership of their part in it.

Another component is VIP support. At every large incident, elected officials have concerns that only personal visits can address. This has the tendency to detract from the incident commander's attention and time. The FIM will be responsible for supporting VIPs at the incident, ensuring that they receive update incident information and coordinate media briefings with the PIO.

Adaptable over time–6 The expanded PIO model will be adaptable over time. The system modes provide advantages over the current system by identifying duties and positions that need to be filled.

Integrated into NIMS– 4 Because of the issue of assistants, the expanded PIO violates some of the ICS and NIMS tenants. The issue of integrating the expanded PIO into the NIMS could be problematic.

Effectiveness–6 The expanded PIO will increase effectiveness of the ICS. Due to the increased situational awareness and public information enhancements, effectiveness is expected to increase.

Externalities–4 The expanded PIO may face difficulties due to the span of control, integration into ICS tenants, and NIMS integration. Therefore, there could be additional problems implementing this model.

Cost–4 The costs to change the ICS will be minimal; however, there will be some costs. The application of the expanded PIO will only be necessary in large, complex incidents. Therefore, the basic structure of the ICS will remain the same, with only the PIO structure changed. Basic ICS courses will not require revisions. Additional position descriptions and training to those descriptions will be required.

Political Acceptability–8 The expanded PIO could be politically acceptable. The PIO is required to accomplish many of these functions and this structure gives them the organized capabilities to meet the ICS objectives. The ability to more effectively

communicate with the public makes this model very supportable. The additional functionality of field information and VIP support will off load tasks from the IC and may help generate political support.

As with the expanded Communications Unit, the effort needed to create this change and implement this model will require overcoming institutional lethargy. However, working through established channels, this lethargy may be overcome.

3. Model 3—Creating a Communications Section

This model would create a Communications Section, which would be responsible for all the communication functions of the incident. The strategic changes to the ICS would consolidate all communication functions under the Communication Section Chief. This Section Chief would be responsible for establishing communication networks for voice, video, and data within the incident. In addition, the Communication Section Chief would be responsible for developing the content and providing external communications to the media, elected official, and the public. Inter-incident communication networks will be established and maintained by the Communication Support Branch. Under this branch, various groups, divisions and units may be established to facilitate radio, video, data, and Internet systems. These systems will carry the information content developed by the incident to the necessary end users.

This model would incorporate all the advantages of Model 1 and Model 2. Internal communications would be enhanced by the expansion of the Communications Unit. The three components would function as described previously, with voice, data, and video components. New technologies would be incorporated, creating advantages of instant messaging, Internet capabilities, social media and email. These assets will help the IC develop the situational awareness to create operational plans. Then these same technologies will help disseminate those plans to all responders.

In addition, the expanded PIO will bring all the benefits described. The expanded PIO will be able to create communication channels to the public utilizing newer technologies and social media. This in turn will create stronger information, fostering

trust in the incident command. The expansion of the PIO to a branch under the Communications Section Chief will eliminate the violation of ICS tenants including issues of span of control. The ability to form divisions, groups, and units under the PIO will smooth the ability of the PIO to manage and direct the direct reports.

The creation of a Communications Section under the IC will bring many of the benefits described above, without many of the span of control issues see in the expanded PIO model. The ability to branch the section and allow the PIO to form divisions and groups with ensure that the model fits well within ICS guidelines. The Communications Section will create a stronger internal and external communications function by being elevated to the level of importance equal to operations and planning.

Common Terminology–5 The Communications Section will not impact common terminology. The traditional terms of branch, division, and group supervisor will continue.

Modular Organization–6 The Communications Section will facilitate a modular organization. The ICS organizational structure develops in a modular fashion based on the size and complexity of the incident, and Communications Unit and PIO functions can be expanded as the incident is needed. On smaller, single agency incidents where a single PIO is needed, that role can be filled. In larger incidents, all functions and positions may be filled. At the largest incidents, the full Communications Section with both branches fill may be required.

Management by Objectives–7 The Communications Section will improve on the ability to create and implement management by objectives. Key objectives always involve developing and maintaining internal and external communication networks to ensure responder and public safety. The creation of the Communication Section will facilitate accomplishing those objectives.

Incident Action Planning–7 The Communications Section will facilitate incident action planning. The Section will be capable of developing the internal and public information systems. In addition, the Section has the capability to develop, activate contingency plans.

Manageable Span of Control–7 The Communications Section will improve on the ability to manage the span of control. Currently, both the Communication Unit and PIO do not have the manageable capabilities to expand to meet the needs of a large complex incident. By creating a Communications Section, we are able to create divisions, groups, and units to ensure that the span of control stays within manageable limits.

In addition, the span of control of the IC will not be impacted. Currently, the IC controls three members of the command staff (PIO, Liaison, and Safety) and four members of the general staff (operations, planning, logistics, and finance). The creation of the Communication Section removes the PIO from the command staff and moves it to the general staff.

Incident Facilities and Locations–5 The Communications Section will not have an impact on facilities and locations.

Comprehensive Resource Management–5 The Communications Section will not have an impact on resource management.

Integrated Communications–8 The Communications Section will improve on the structural capabilities to improve communications. By elevating the focus of communication to the level of Section, communication becomes as important as operations. This function will need to be addressed, on every incident, alongside of strategic and tactical operations.

Establishment and Transfer of Command–6 The Communications Section will not affect the establishment or transfer of command. However, with the establishment of the Section, the internal transfer of command may be facilitated.

Chain of Command and Unity of Command–6 The Communications Section will not affect the chain of command. However, with the establishment of the Communications Section, the internal chain of command may be facilitated.

Unified Command–5 The Communications Section will not impact the chain of command.

Accountability–5 The Communications Section will not impact the accountability.

Dispatch/Deployment–5 The Communications Section will not impact dispatch and deployment.

Information and Intelligence Management–8 The Communications Section will greatly enhance information and intelligence. The expanded Communication Unit will develop and maintain internal communication networks for voice, data, and video. This will enhance internal information management. The expanded PIO will improve the ability to reach out to media, social media, and the Internet to create additional capabilities and resources to gain situational awareness. The expanded PIO's ability to keep field members informed through new technologies will also help information flows.

Adaptable to any Emergency–6 The Communications Section will adapt to any size incident. At single agency events, the single PIO will continue to serve. The communication Unit will be filled as necessary. As the incident grows, positions in the Communications Section can be filled.

Adaptable to any Agency–5 The Communications Section will be adaptable to any agency.

Expandable–7 As stated above, the Communications Section will be expandable. The model system is more capable of expansion than the current model.

Adaptable Over Time–6 The Communications Section will be adaptable over time. The system modes provide advantages over the current system by identifying duties and positions that need to be filled.

Integrated into NIMS-8 The Communications Section will adapt into NIMS well. The Section will meet the NIMS requirements and guidelines. The Section will help remove some issues, as stated, with the current deployment of assistant PIO.

Effectiveness–7 The Communications Section will increase effectiveness. By elevating the communication function to equal operations, the signal will be sent that internal and external communications are issues the IC must consider from the start. The addition of the expanded Communication Unit and expanded PIO will increase effectiveness.

Externalities–4 The external issues facing creating a Communication Section are large. Inherent lethargy could stall the process. Although the Communications Section could be shown to be an advantage, the obstacles are there.

Cost–2 The Communications Section will require the greatest cost of the three models. The basic structure of the ICS will require modification, new training curriculum will need to be developed, and all manuals will require revisions. This is not a minor factor.

Political Acceptability–3 Due to the fundamental change to the ICS, this model will face the largest political headwinds. Changing the ICS to include a Communications Section is the most ambitious of the models. However, it also offers the most benefits. The ICS has grown throughout the world and changed due to catastrophic incidents. However, the ICS should not wait until events force the change.

Ahlstrand et al. have stated, "A shared commitment to beliefs encourages consistency in an organization's behavior, and thereby discourages changes in strategy. Before strategic learning can occur, the old [dominant] logic must in a sense be unlearned by the organization. [149] In the case of the recommendation, unless we are met with a significant event that clearly displays the benefits of the recommendations, change will require efforts.

[149] Bruce Ahlstrand, Henry Mintzberg, and Joseph Lampel, *Strategy Safari*. Kindle. New York: Simon & Schuster, Inc, 2001.

The Incident Command System has been developed and adapted because of "Black Swans" and other significant events. The Incident Command System was developed in Southern California as a result of the catastrophic wildland fire siege of 1970. [150] It began to spread throughout the fire service in California from south to north. Then another disaster struck. As a result of the East Bay Hills Fire on Saturday, October 19, 1991, in Oakland, the California legislature passed a law requiring the use of ICS for all public safety agencies in California.[151] ICS was slowly being adapted by other agencies across the United States, including federal agencies, when the September 11, 2001, attacks occurred. The 9/11 Commission Report stated that the ICS needed to be the national standard[152] and, in February 2003, President Bush issued Homeland Security Presidential Directive (HSPD) 5. HSPD 5 directed the Secretary of the Department of Homeland Security to develop and administer a National Incident Management System (NIMS). ICS has been growing in understanding and utilization since then. The events of Katrina, Irene and Deepwater Horizon have continued the spread in the United States.

Due to similar emergency incident management problems, Australia developed the Australasian Inter-Service Incident Management System (AIIMS). The system developed by the Australian Association of Rural Fire Authorities was based on the United States ICS with modifications to suit the Australian environment. One of the most significant of these was to call the core operational component of the AIIMS, the Incident Control System, in contrast to the North American Incident Command System.[153]

The Australian Incident Control System was extremely tested with the Black Sunday Brushfires, a series of brushfires that burned across the Australian state of

---

150 "History of ICS," National Wildland Coordinating Group, National Training Curriculum, October 1994. Available at http://www.nwcg.gov/pms/forms/compan/history.pdf.

151 "Standardized Emergency Management System," California Code of Regulations, Title 19, Division 2, Chapter 1. Available at http://www.vetmed.ucdavis.edu/vetext/danr/danrguide2_33-38sems.pdf.

152 "*9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*," New York: W. W. Norton & Company, 2004. 11.

153 Australasian Fire and Emergency Service Council, *The Australasian Inter-Service Incident Management System*. Third ed., 2011.

Victoria on Saturday, February 7, 2009. The fires occurred during extreme weather conditions, and resulted in Australia's highest ever loss of life from a bushfire; 173 people died and 414 were injured. [154]

In April 2009, Premier John Brumby announced that there would be a Royal Commission into the fires, which would examine "all aspects of the government's bushfire strategy." The Commission therefore examined the policies, systems, and structures needed to ensure that government, fire and emergency service agencies and individuals make informed, effective decisions about their response to brushfires in a way that protects life and minimizes loss.[155]

The recommendations of the Commission included a plan to enhance external communications in the AIIMS. Recommendation 14 stated, “The Victorian fire agencies amend the AIIMS framework before the 2010–2011 fire season in order to designate the Information Unit as a separate section reporting directly to the Incident Controller and require that the Information Unit contain a dedicated Public Information Officer whenever a full incident management team is required. [156]

The analysis shows that internal (incident communications) and external communications (public information) related sufficiently so that they can be combined within the ICS. The Communications Unit develops the communications systems with the incident while the expanded PIO will develop additional value-added content for those systems. The two functions of internal and external communications can be consolidated into a single section to gain efficiencies.

ICS provides a flexible core mechanism for coordinated and collaborative incident management, whether for incidents where additional resources are required or are provided from different organizations within a single jurisdiction or outside the jurisdiction, or for complex incidents with national implications. Incident management

154 “Final Report,” 2009 Victoria Brushfires Royal Commission,” August 2009. http://www.royalcommission.vic.gov.au/Commission-Reports/Final-Report.

155 Ibid.

156 Ibid.

approaches are the fulcrum of an Information Age transformation; understanding command and control is among the most important and urgent tasks we have on the critical path to transformation and the ability to meet twenty-first century challenges.

A critical piece of command and control is communications. Within the structure of the ICS, communications has been identified as weaknesses, and alternative models have been designed. The analysis and trade-offs of each model has been discussed in order to identify the best possible recommendation to support.

The final chapter presents a summary of the assessments and the final recommendations. In addition, further areas of study are outlined.

VII. FINAL RECOMMENDATIONS

A. INTRODUCTION

Chapter VII l summarizes the models and presents the findings, which include the summary of each of the key components and present the recommendations. In addition, this chapter identifies areas of further study.

The ICS allowed Southern California wildland fire protection agencies to "make a quantum jump" in their capabilities and ability to effectively coordinate interagency action and in the allocation of resources in dynamic, multiple-fire situations. Since then, ICS has spread throughout the United States and to other countries. While being adopted by other agencies, the ICS has gone through a maturation process. ICS has been assessed and modified to make the system work more effectively and efficiently in all-hazards incidents. This process continues today. Part of this process is the constant review of incidents and events where ICS was utilized to gather the lessons learned and question whether the current state is the best possible configuration.

Based on assessments and after action reports from incidents, communication is mentioned as one of the areas that fail most often. Internal communications, the ability of situational awareness to get to the IC and the commander's orders and intent to get to the responders in the field, has failed numerous times. External communications (public information) has failed to inform the communities of the size and scope of the incident. In addition, new technologies are pushing current communication capabilities beyond the ICS structure. The research questions that were studied were:

1. Which type of structure would make communications in the ICS more efficient?

2. Are internal (incident communications) and external communications (public information) related sufficiently so that they can be combined within the ICS?

3. Or, do internal and external communications need to remain separated to operate efficiently?

4. Would changing the ICS communications structure meet the community's current expectations?

In order to focus the research and discuss the questions, a Soft systems methodology was utilized. Soft systems methodology with its systemic approach for tackling real-world problematic situations works well in this situation. Three theoretical models were designed that could improve the ICS and reduce or eliminate the communication issues. The first model expanded the Communication Unit within the Logistics Section. The expansion included new technologies for communication and incorporated them into the ICS structure. These technologies include data, video, and Internet. The tactics of these technologies include instant messaging, email social media, and web-enabled applications. Through these technologies, additional lines of communication can be opened, maintained, and utilized to increase communication. These technologies can reduce the friction of current systems and create a stronger situational awareness for all members.

The second model focused on external communications and the Public Information Officer. This model expanded the PIO and defined the positions to accomplish the duties and responsibilities of the PIO. In addition, the model included the use of new technologies to facilities communication with the communities involved. As seen in recent events, the use of technology to send and receive important information is happening and is going to grow in the future. This model realized this and incorporates that into the ICS structure. Sensing information from nontraditional sources and pushing information out using social media will be invaluable for the IC in the future. The methods enabled with the expanded PIO will open lines of communication, creating flowing information. The result will be a stronger trust in the incident.

The third model discussed combines the internal and external communication functions into a Communications Section working directly for the IC. This creates a fifth section alongside Operations, Planning, Logistics, and Finance. This elevates communication to equal importance. By this alone, communication becomes of primary importance to the IC. In this model, the structures and advantages of the expanded

Communications Unit and the expanded PIO model can be maintained. The expanded Communications Unit, with new technology capabilities and the expanded PIO can be incorporated. Therefore, the described advantages of both can be realized. The Communications Unit will be responsible for developing voice, data, and video networks for the incident, and the PIO will develop the content for those networks. The internal and external communication functions will work under a common supervisor to create a stronger system.

1. Findings

The data analysis shows that the option of creating a Communication Section would offer the most benefit. However the other options also offer some improvements over the current structure.

The analysis showed that the expanded Communications Unit offered great improvements in the areas of integrated communications and intelligence, and information management. In addition, the factor of information flows to and from the incident commander displayed improvements. Of the three options, this model and the expanded PIO model showed the greatest offer of political acceptability.

The expanded Communications Unit will be responsible for developing and maintaining new technologies, including Internet and email, data, instant messaging and global information systems. The research found the benefits of these systems would outweigh the expected costs. It does not seem unreasonable to assume that products relating to the situational awareness would improve the quality of incident command. It is expected to lead to a more disciplined, yet more creative, awareness process. The ability to provide a clearer input to the planning function would facilitate the development of operational plans.

Therefore, emerging technologies will greatly enhance the ability of controlling a incident, monitoring the situation, developing situational awareness, developing courses of action, decision making that selects among the courses of action, developing and promulgating guidance to implement those decisions, and establishing mechanisms for

feedback that allow the cycle to be continuous by monitoring the situation during implementation. The expanded Communication Unit will be staged to implement the new technologies will be essential in meeting these steps.

The analysis showed that of the three models, the expanded PIO role offered the least improvement in the 14 key components. This is mainly due to the chain of command issue discussed. However, the expanded PIO role also offered great improvements in the areas of integrated communications and intelligence and information management. The expanded PIO will facilitate information flows to the incident commander and from the IC to the field resources. The research found the utilization for new technologies of instant messaging; the PIO has the capability of developing overall situational awareness.

The research found the expanded PIO will greatly improve external communication and information flows. The ability to monitor web sites, media reports, and social media will rise and assist the PIO of developing greater situational awareness. That awareness will be forwarded to the Planning Section for incorporation into operational plans. In addition, the utilization of social media's two-way communications to facilitate information flows will quickly create additional communication channels to get the incident commanders message to the communities affected. The research found that the ability to deliver the size, scope, impact, and warnings can be distributed instantaneously. The effectiveness of the ICS will be increased due to increased situational awareness of the responders, stakeholders, and the communities impacted.

The expanded PIO could be politically acceptable. The PIO is required to accomplish many of these functions and this structure gives them the organized capabilities to meet the ICS objectives. The ability to more effectively communicate with the public makes this model very supportable. The additional functionality of field information and VIP support will off load tasks from the IC and may help generate political support. However, the research found that the expanded PIO model has issues with span of control and ICS rank. The problem of the PIO having multiple assistant PIOs creates concerns for many in the ICS community. These may be obstacles in

moving this model forward. Institutional lethargy is another major hurdle. Making changes to the ICS, less than ten years since its implementation, may prove difficult

The costs to change the ICS will be minimal; however, there will be some costs. The application of the expanded PIO and Communications Unit will be necessary only in large, complex incidents. Therefore, the basic structure of the ICS will remain the same, with only the internal Communication Unit and PIO structure changed. Basic ICS courses will not require revisions. Additional position descriptions and training to those descriptions will be required.

The analysis showed that creating a Communication Section would offer the most improvement in the 14 key components. Creating a Communication Section offers great improvements in the areas of integrated communications and intelligence and information management. In addition, information flows would be enhanced.

The Communication Section model would incorporate all the advantages of expanded Communication Unit and the expanded PIO. Internal communications would be enhanced by the expansion of the Communications Unit. The three components would function as described previously, with voice, data, and video components. New technologies would be incorporated, creating advantages of instant messaging, Internet capabilities, social media, and email. These assets will help the IC develop the situational awareness to create operational plans. Then these same technologies will help disseminate those plans to all responders. However, the cost and political acceptability of this model weighs it down.

2. Recommendation

The research found that the creation of the Communication Section would provide the most benefits towards improving communications in the ICS. The section brings the benefits of both other models while eliminating some of the potential criticisms.

However, expanding the existing communications and PIO functions can be displayed as a minor change, consolidating functions and adding capabilities within themselves. One finding is that the expanded Communications Unit and the expanded

PIO are not necessarily mutually exclusive and may be in fact accomplished in tandem. The benefits of the Communication Unit developing the network and the expanded PIO delivering the content may be supportable. The model of creating a Communication Section may be to be difficult to overcome due to resistance to strategic change. The political will for creating a Communication Section may not exist at this time.

By reviewing the Australian model, the research found that change can happen. Unfortunately, we should not wait for a catastrophic incident with a failure of the ICS to generate the political will to change. We should not need another 9/11 Commission or something similar to the Royal Commission to mandate that the communication be given a higher significance in the ICS.

The recommended changes will take an expected route to implementation. The recommendations will be introduced at the NIC, FIRESCOPE and NIMS Consortium simultaneously. Education discussions and public comment will follow. Without serious opposition, the recommendations may be included in the next set of changes heading out of the Consortium and FIRESCOPE to the NIC. At the NIC, the education discussions and public comment will be repeated. While there is anecdotal support from many larger public safety organizations, primarily agencies with significant public information offices, smaller agencies have not embraced the need yet.

The wild card will be an event of national significance. When we experience an event of national significance, and if we show unnecessary damage, life loss, or delay of response, the public will demand an inquiry. Much like the 9/11 commission and Australia's Royal Commission, the findings may point to communications as a contributing factor. When this happens, these recommendations may be pushed forward. Implementation of these changes may be mandated as a result.

Adoption of the incident command system has been a disruptive innovation. The organized structure of incident management has revolutionized response. The consistent methods have streamlined the integration of multiple public safety agencies into one system. The recommended changes will be an incremental change to the ICS. Creating a Communications Section combines the tasks of internal and external communication into

a single section. The modified ICS structure will maintain the same span of control, and supervisory reporting procedures will be little changed.

In the annual update there is a struggle between the need for continuity and the need to adapt to a changing environment. As time passes, we learn, and thus both the national emergency management organization and the trends will slowly change. Therefore, there is a constant need to continue the change momentum, replace trends, but also to change their names to meet current descriptions and indicators.

3. Areas of Further Study

While the existing model of maintaining the status quo is not formally evaluated, that option could remain if expected benefits do not reach a significant return of investment. This option would not alter the ICS, but may utilize other methods to support communications. This would entail expanding the training and implementation process of the ICS, Communication Unit and Public Information Officer to ensure that all incident communication functions can be carried out. The observations from previous incidents of national significance makes the solution of maintaining the current ICS structure less than desirable from a homeland security and response perspective. One rather dubious advantage with this option is that it will almost certainly allow for the documentation of ICS communications issues, which will further substantiate the need for a different policy option.

4. Conclusion

Discussion and education on the recommendation could be protracted. Unfortunately, the recommendation is not testable and cannot generate objective, measurable results, such as improved response times or less dropped radio messages. Therefore, the recommendation may have difficulty proving the necessity for change, until the ICS fails at a critical incident. When this happens, citizens are going to demand changes, and this recommendation will provide answers to the hard questions the public is going to be asking the public safety professionals. However, the nation should not wait for the system to fail. It must be proactive in identifying areas of improvement, soliciting

counsel and implementing changes that will benefit the stakeholders. Significant incidents have driven the development of the ICS; the nation must not wait for another significant incident to make these changes.

BIBLIOGRAPHY

9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States." New York: w.w. Norton & Company, 2004.

"About FIRESCOPE." Available at http://firescope.org/about-us.htm.

Ahlstrand, Bruce; Henry Mintzberg, and Joseph Lampel. *Strategy Safari*. Kindle. New York: Simon & Schuster, Inc, 2001.

"AirDisaster.Com: Special Report: PSA Flight 1771,"Available at http://www.airdisaster.com/special/special-pa1771.shtml.

Alberts, David S. and Richard E. Hayes. "Power and Control: Command and Control in the Information Age," Available at http://www.dodccrp.org/files/Alberts_Power.pdf."

Attorney-General's Department Disasters Database: Black Christmas Brushfire." Available at. http://www.disasters.ema.gov.au/Browse%20Details/DisasterEventDetails.aspx?DisasterEventID=1320.

"Attorney-General's Department Disasters Database." Available at http://www.em.gov.au/Resources/Pages/DisastersDatabase.aspx.

"Australasian Fire Authorities Council: Knowledge Web." Available at http://knowledgeweb.afac.com.au/aiims.

Australasian Fire and Emergency Service Council. *The Australasian Inter-Service Incident Management System*. Thrid ed., 2011.

Barrantes, S. A., M. RodrIguez, R. Pérez. "Information Management and Communication in Emergencies and Disasters." Pan American Health Organization, 2009. Available at http://www.allindiary.org/pool/resources/4-2-im-commguide-responseteams-paho-2009.pdf.

"Beyond Katrina Improving Disaster Response Capabilities.pdf," n.d. file:///C:/Users/chdsstudent/Documents/Naval%20Post%20Grad/Thesis/Crtitcisms/Beyond%20Katrina%20Improving%20Disaster%20Response%20Capabilities%20PRINTED.pdf.

"Black Friday - Royal Commission - Judge's Findings - The Fire," *ABC News Australia*. Available at http://www.abc.net.au/blackfriday/royalcommission/index_findings.htm.

Buck, Dick A., Joseph E. Trainor, and Benigno E. Aguirre. “A Critical Evaluation of the Incident Command System and NIMS.” *Journal of Homeland Security and Emergency Management* , no. 3 (2006). Available at http://www.bepress.com/jhsem/vol3/iss3/1.

Busari, Stephanie. “Tweeting the Terror: How Social Media Reacted to Mumbai" *CNN World* November 27, 2008. http://articles.cnn.com/2008-11-27/world/mumbai.twitter_1_twitter-tweet-terror-attacks?_s=PM:WORLD.

“California Department of Forestry and Fire Protection - *Esperanza Fire*," Available at http://bof.fire.ca.gov/incidents/incidents_details_info?incident_id=161.

“California Department of Forestry and Fire Protection - *The Witch Fire*,” Available at. http://cdfdata.fire.ca.gov/incidents/incidents_details_info?incident_id=225.

“Cedar Fire" San Diego Fire-Rescue Department. Available at http://www.sandiego.gov/fire/about/majorfires/2003cedar.shtml.

Chandler, Raymond. "*Red Wind*,” Available at http://www.ae-lib.org.ua/texts-c/chandler__red_wind__en.htm.

Checkland, Peter. *Systems Thinking, Systems Practice*. New Jersey: John Wiley & Sons, 1999.

———. “Achieving ‘Desirable and Feasible’ Change: An Application of Soft Systems Methodology,” *Journal of the Operational Research Society.* Vol 6, No 9, 1985. 821-831 Available at http://www.palgrave-journals.com/jors/journal/v36/n9/pdf/jors1985148a.pdf.

Checkland, Peter, John Poulter. *Learning for Action: A Short Definitive Account of Soft Systems Methodology, and Its Use Practitioners, Teachers and Students*. New Jersey: Wiley, 2007.

Christen, Hank, Paul Maniscalco, Alan Vickery, and Frances Winslow. “An Overview of Incident Management Systems,” September 2001, Available at http://www.hcanj.org/docs/An_Overview_of_Incident_Management_Systems.pdf.

Cole, Dana. “The Incident Command System:A 25-Year Evaluation by California Practitioners.” National Fire Academy, February 2000. Available at http://www.hsdl.org/?view&doc=45746&coll=limited.

“Commandant Instruction 3120.14.” United States Coast Guard. Available at http://www.uscg.mil/directives/ci/3000-3999/ci_3120_14.pdf.

Committee on Homeland Security: Hearings on Preliminary the Lessons from Deepwater Horizon. 111th Cong. (2010). September 22, 2010. Serial No. 111–80. Statement of Mr. Craig Paul Taffaro, Jr., St. Bernard Parish, Louisiana.

Committee on Homeland Security, Subcommittee on Emergency Preparedness, Response, and Communications. Hearings on Communicating with the Public During Emergencies, 112th Cong. (2010) July 8, 2011**.** Available At Https://Www.Hsdl.Org/?View&Did=489262.

"Deepwater Horizon." National Oceanic and Atmospheric Administration. Available at http://www.noaa.gov/deepwaterhorizon/.

Department of Homeland Security. "National Incident Management System," 2004.

———. "National Incident Management System," 2008. Available at http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf.

———. "National Response Framework," 2008. Available at http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf.

———. "National Response Plan," 2004. Available at http://www.it.ojp.gov/fusioncenterguidelines/NRPbaseplan.pdf.

———. "The First Year After Hurricane Katrina: What the Federal Government Did," n.d. Available at http://www.dhs.gov/xfoia/archives/gc_1157649340100.shtm.

Emmons, Steve. "Brush Fires Sweep Trabuco, Brea Areas, Force Evacuation: Shifting Winds Ease Threat in County After Flames Scorch Campgrounds, Raze Home, Peril Gasoline Plant." *Los Angeles Times*, September 28, 1970, sec. PART II.

"Federal Response Plan." *Public Law 93-288 as Amended 1992*, n.d. http://library.findlaw.com/1992/Apr/1/127810.html.

"Final Report." 2009 Victoria Brushfires Royal Commission," August 2009. http://www.royalcommission.vic.gov.au/Commission-Reports/Final-Report.

"Fire Burns in Espraranza." *Los Angeles Times*, September 27, 1889, sec. A.

"The First Interstate Bank Fire." *Disaster Recovery Journal* Available at http://www.drj.com/drworld/content/w1_119.htm.

"The First Year After Hurricane Katrina: What the Federal Government Did." Department of Homeland Security. n.d. Available at http://www.dhs.gov/xfoia/archives/gc_1157649340100.shtm.

Gecowets, Gregory A. S *and* Marquis, Jefferson P. “Applying the Lessons of Katrina,” *Joint Forces Quarterly* Issue 48, 1st quarter 2008. Available at http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA518742. 70–76.

Greenwood, Ronald G. “Management by Objectives: As Developed by Peter Drucker, Assisted by Harold Smiddy,” *Academy of Management. The Academy of Management Review (pre-1986);* April 1981; 6.

“History of ICS.” National Wildland Coordinating Group, National Training Curriculum, October 1994. Available at http://www.nwcg.gov/pms/forms/compan/history.pdf.

“Homeland Security Presidential Directive 5.” Available at http://www.hsdl.org/?view&doc=82670&coll=limited.

Howitt, Arnold M., and Herman B. Leonard. “A Command System for All Agencies?” *Crisis/Response Journal*, March 2005, 40–42.

———. "Beyond Katrina: Improving Disaster Response Capabilities" *Crisis/Response Journal.* September 2006.

"Hurricane Katrina.” “National Oceanic and Atmospheric Administration. Available at http://www.katrina.noaa.gov/.

“Laguna Fire 1970 - One of California’s Worst Wildfires.” Available at http://www.cccarto.com/cal_wildfire/laguna/fire.html.

Lester, Stan. “Soft System Methodology,” April 2008. Available at http://www.sld.demon.co.uk/ssm.pdf.

“The Los Angeles Fire Department Historical Society- *The Bel Air Fire - Nov. 6th, 1961*.” Available at http://www.lafdmuseum.org/siteblog-post-action/id.22/title.the-bel-air-fire-nov-6th-1961.

“Major Incident Procedure Manual.” London Emergency Services Liaison Panel. TSO (The Stationery Office), 2007. Available at www.tsoshop.co.uk.

Mats Lindgren, and Hans Bandhold. *Scenario Planning: The Link Between Future and Strategy*. New York: Palgrave Macmillan, 2003.

Matthew, David, and Thomas A. Maloney. “The Application of the National Incident Management System In Law Enforcement Operations,” National Incident Management System Consortium. July 2009. Available at http://www.ims-consortium.org/NIMSC_White_Paper_Final_Version.pdf.

Meier, Kenneth M., and John Bohte. “Span of Control and Public Organizations: Implementing Luther Gulick’s Research Design.” *Public Administration Review* 63, no. 1 (February 2003): 61.

Moody, Theodore J. “Filling the Gap Between Nims/Ics and the Law Enforcement Initial Response in the Age of the Urban Jihad.” Master's Thesis, Naval Postgraduate School, 2010), http://www.dtic.mil/dtic/tr/fulltext/u2/a531492.pdf.

“National Incident Management System Consortium." Available at http://www.ims-consortium.org/backinfo.htm.

National Integration Center (NIC). Incident Management Systems Integration Division. “National Incident Management System (NIMS): Five-Year NIMS Training Plan,” 2008. Available at http://www.nema.ne.gov/pdf/fy08-nims-5yearplan.pdf.

Neville, William M., and Robert Neamy. “The Evolution of the National Incident Management System.” *Fire Rescue Magazine*, August 2011.

Oklahoma Department of Civil Emergency Management. “After Action Report: Alfred P. Murrah Federal Building Bombing,” n.d.

“Old Fire 10-26-03.” Available at http://www.incidentcontrol.com/oldfire/index.html.

“Past Present Future.pdf.” Available at http://firescope.org/firescope-history/past%20present%20future.pdf.

Quarantelli, E. L. “Disaster Planning, Emergency Management, And Civil Protection: The Historical Development And Current Characteristics Of Organized Efforts To Prevent And To Respond To Disasters.” *Disaster Research Center*, 1998.

Rowley, Dale D. “The Fires That Created an IMS.pdf,” Available at. http://www.uninets.net/~dsrowley/The%20Fires%20that%20Created%20an%20IMS.pdf.

Sager, Bill. “Command Confusion,” *Wildfire Magazine*. Available on-line at http://wildfiremag.com/command/command_confusion/.

“Santa Ana Winds - Wildfires" National Oceanic and Atmospheric Administration. Available at http://www.noaawatch.gov/2008/santa_ana.php.

“Some Highlights of the Evolution of the Incident Command System.” Available at http://www.firescope.org/firescope-history/Some%20Highlights%20of%20the%20Evolution%20of%20the%20ICS.pdf.

Smith, Duane M. “A Study of Command and Control of Multi-Agency Disaster Response Operations.” (Doctoral Thesis, University of Phoenix, December 2010) Available at http://pqdtopen.proquest.com/#viewpdf?dispub=3467495.

Smith, Patrick C., and David M. Simpson. “The Role of Mobile Emergency Tactical Communication Systems for Disaster Response,” 2005. Available at http://hazardcenter.louisville.edu/pdfs/wp0605.pdf.

“Standardized Emergency Management System.” California Code of Regulations, Title 19, Division 2, Chapter 1. Available at http://www.vetmed.ucdavis.edu/vetext/danr/danrguide2_33-38sems.pdf.

Torgerson, Dial. “14 Major Fires Rage Out Of Control: 256 Homes Destroyed as Flames Burn 180,000 Acres Some Fight It or Flee It---Others Just Yell Fore! Man Vs. Nature at Her Worst.” *Los Angeles Times*, September 27, 1970, sec. A.

———. “Can We Prevent Future Disasters?” *Los Angeles Times*, October 4, 1970, sec. A.

“Unit 7 - Fireground Command,” John Jay College of Criminal Justice. Available at. http://web.jjay.cuny.edu/~tflan/documents/101docs/FIS101FiregroundCommand.pdf.

United States Fire Administration/Technical Report Series. “*The East Bay Hills Fire*,” Available at http://www.usfa.fema.gov/downloads/pdf/publications/tr-060.pdf.

United States Fire Administration. “*America Burning*,” September 7, 1972, Available at http://www.usfa.fema.gov/downloads/pdf/publications/fa-264.pdf.

“Urban Search and Rescue (US&R).” Federal Emergency Management Agency. Available at http://www.fema.gov/emergency/usr/.

Wallop, Harry. “Japan Earthquake: How Twitter and Facebook Helped" *The Telegraph*, March 13, 2011. http://www.telegraph.co.uk/technology/twitter/8379101/Japan-earthquake-how-Twitter-and-Facebook-helped.html.

“Weather.” *Los Angeles Times*, September 22, 1970, sec. Part II.

“Weather Service Glossary.” "National Oceanic and Atmospheric Administration, Available at http://www.weather.gov/glossary/index.php?word=red%20flag%20warning.

Wenger, Dennis, E. L. Quarantelli, and Russell R Dynes. “Disaster Analysis: Police and Fire Departments.” *Disaster Research Center*, 1989.

———. “Is the Incident Command System a Plan for All Seasons and Emergency Solutions.” *Hazard Monthly*, May 1990.

Yates, Julian. “Improving the Management of Emergencies: Enhancing the ICS.” *Australian Journal of Emergency Management* 14, no. 2 (Winter 1999): 22–28.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX. KEY COMPONENTS

System Requirement	Model 1 Expanded Communications Unit	Model 2 Expanded PIO	Model 3 Communications Section
Common Terminology	5	5	5
Modular Organization	6	6	6
Management by Objectives	7	7	7
Incident Action Planning	6	6	7
Manageable Span of Control	6	3	7
Incident Facilities and Locations	5	5	5
Comprehensive Resource Management	6	5	6
Integrated Communications	8	6	8
Establishment and Transfer of Command	5	5	5
Chain of Command and Unity of Command	5	5	5
Unified Command	5	5	5
Accountability	5	5	5
Dispatch/Deployment	5	5	5
Information and Intelligence Management	8	8	8

Table 4. Key Components Results

System Requirement	Model 1 Expanded Communications Unit	Model 2 Expanded PIO	Model 3 Communications Section
14 goals and key components (From above)	5.86	5.43	6.00
Information flow to IC and field	8	8	8
Information flow to (and from) citizens	6	8	8
Adaptable to any emergency	5	6	6
Adaptable to any Agency	4	4	5
Expandable	7	7	7
Adaptable over time	5	6	6
Integrated into NIMS	5	4	8
Effectiveness	7	6	7
Cost	7	4	2
Externalities	6	4	4
Political Acceptability	8	8	3

Table 5. Adaptability Criteria and Criteria Measuring Success Results

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Nadav Morag
   Naval Postgraduate School
   Monterey, California

4. Roxanne Bercik
   Los Angeles Fire Department
   Los Angeles, California

5. Bob Neamy
   NIMS Consortium
   Gardnerville, Nevada

6. National Integration Center
   FEMA
   Washington, DC